VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Systémy platebních bran a jejich aplikace v prostředí kryptoměn

Payment Gate Systems and Their Application in Cryptomime

2019 Bc. Martin Wójcikiewicz

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Martin Wójcikiewicz**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Systémy platebních bran a jejich aplikace v prostředí kryptoměn
Payment Gate Systems and Their Application in Cryptomime

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem práce je analyzovat a implementovat platební bránu, která bude přijímat různé druhy kryptoměn. Brána bude akceptovat nejen významné kryptoměny (Bitcoin, Litecoin, Ethereum), ale i tzv. altcoiny (alternativní kryptoměny). Cílem je tuto bránu integrovat jako alternativní možnost úhrady platby formou kryptoměn. Platební brána bude umět přijímat kryptoměny, a následně je konvertovat na jiné, včetně klasických měn (CZK, EUR, USD, GBP). Dále bude poskytovat tzv. inteligentní kurzovní lístek, který bude prezentovat aktuální kurzy kryptoměn se zohledněním poplatků a směnných kurzů za převody, tak aby byly minimalizovány možné ztráty způsobené kolísáním kurzů a konverzními poplatky.
1. Student provede analýzu existujících řešení pro platby formou kryptoměn (například Bitcoin Pay). Dále student analyzuje a popíše funkce a principy fungování klasických platebních bran (GoPay, PayU a další).
2. Student se seznámí s API, které poskytují světové burzy a tržiště kryptoměn a na jejich základě vystaví infrastrukturu pro příjem, konverzi a výplatu plateb v kryptoměnách.
3. Student analyzuje požadavky na platební bránu, která by akceptovala různé druhy kryptoměn, dynamicky generovala kurzovní lístky včetně vyčíslení konverzních nákladů, přijímala platby v kryptoměnách a doručila je v požadované měně na účet žadatele o platbu.
4. Rovněž se student zaměří na popis legislativního rámce v České Republice a EU ve vztahu k přijímání plateb za produkty a služby v kryptoměnách.
5. Na základě vybraných technologií a dostupných API student provede analýzu, návrh a implementaci platební brány, která bude kombinovat on-line aplikaci i API rozhraní pro platební transakce.
6. Student provede demonstrativní nasazení platební brány do zvolené platformy pro eshopy, opensource prodejního rozšíření redakčního systému nebo prodejního tržiště.
7. Výstupem práce bude také metodická příručka jak pracovat s kryptoměnami v rámci elektronické komerce a jak integrovat tuto platební bránu do vlastního prodejního řešení.
8. V závěru student provede srovnání dosažených výsledků s referenčními projekty a navrhne možnosti dalšího rozšíření.

Seznam doporučené odborné literatury:

[1] GORMLEY, Clinton a Zachary TONG. Elasticsearch: the definitive guide. ISBN 1449358543.
[2] SHKLAR, Leon. a Rich. ROSEN. Web application architecture: principles, protocols and practices. 2nd ed. Hoboken, NJ: Wiley, c2009. ISBN 047051860x.
[3] SHIVAKUMAR, Shailesh Kumar. Architecting high performing, scalable and available enterprise web applications. ISBN 9780128022580.
[4] WEERAWARANA, Sanjiva. Web services platform architecture: SOAP, WSDL, WS-Policy, WS-Addressing, WS-BPEL, WS-Reliable Messaging, and more. Upper Saddle River, NJ: Prentice Hall PTR,

c2005. ISBN 0131488740.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Radoslav Fasuga, Ph.D.**

Datum zadání: 01.09.2018

Datum odevzdání: 30.04.2019

doc. Ing. Jan Platoš, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 23. dubna 2019 .....

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava.

V Ostravě 23. dubna 2019 .....

Rád bych na tomto místě poděkoval za pomoc při vypracovávání této práce, panu Ing. Radoslavu Fasugovi, Ph.D., a také svým přátelům a rodině za podporu.

Abstrakt

Tato diplomová práce obsahuje analýzu a implementaci platební brány, která přijímá kryptoměny Bitcoin, Litecoin, Ethereum, Ripple, DASH a NEO.

V úvodu se práce zabývá principem fungování kryptoměn, bezpečností v rámci kryptoměn, dostupnými burzami a trhem s kryptoměnami, klasickými a krypto platebními branami nebo legislativním rámcem ve vztahu ke kryptoměnám v České republice a EU.

Druhá část práce je věnována implementaci. Tato část obsahuje popis platební brány, popis implementace, popis využití REST API burzy Binance a směnárny Coinbase, včetně ukázek z kódu aplikace. Následně obsahuje implementaci šesti podporovaných kryptoměn v rámci aplikace, a v závěru popisuje vytvořenou aplikaci a její zabezpečení.

Vytvořenou aplikaci je po možno využít v případě e-shopu jako platební variantu. Popřípadě je také možno aplikaci využít jako samostatný produkt nabízený veřejnosti.

Klíčová slova: kryptoměny, bitcoin, litecoin, ethereum, dash, neo, ripple, platební brána, binance, coinbase, asp.net core, paypal, gopay

Abstract

This thesis contains an analysis and implementation of a gateway which accepts cryptocurrencies Bitcoin, Litecoin, Ethereum, Ripple, DASH and NEO.

Introduction is focused on principles of functioning of the cryptocurrencies, their safety, available stock exchanges and a market with cryptocurrencies, common and crypto gateways or legislative framework in regard to cryptocurrencies in the Czech republic and EU.

The second part of the thesis is dedicated to implementation. This part contains description of a gateway, description of implementation, usage of REST API stock exchange Binance and exchange office Coinbase including examples of codes from the application. Follows implementation of six supported crypto currencies in regard to the application. Conclusion focuses on the created application and her safety.

The created application might be used in case of e-shops as a payment method. Eventually the application might also be used as a single product for sell.

Key Words: cryptocurrencies, bitcoin, litecoin, ethereum, dash, neo, ripple, payment gateway, binance, coinbase, asp.net core, paypal, gopay

Obsah

Seznam použitých zkratek a symbolů **10**

Seznam obrázků **11**

Seznam tabulek **12**

Seznam výpisů zdrojového kódu **13**

1 Úvod **15**

2 Kryptoměny **16**
2.1 Co je to kryptoměna? . . . 16
2.2 Jak kryptoměnu získat? . . . 17
2.3 Bitcoin . . . 19
2.4 Alternativní kryptoměny . . . 20

3 Bezpečnost **30**
3.1 Jsou kryptoměny bezpečné? . . . 30
3.2 Jak se chránit? . . . 31
3.3 Anonymita . . . 32

4 Burzy a trh **33**
4.1 Burzy kryptoměn . . . 33
4.2 Poplatky a omezení . . . 34
4.3 Trh s kryptoměnami . . . 36

5 Klasické platební brány **37**
5.1 GoPay . . . 37
5.2 PayPal . . . 38

6 Krypto platební brány **39**

7 Legislativní rámec ve vztahu ke kryptoměnám **40**
7.1 V České Republice . . . 40
7.2 V Evropské unii . . . 41

8 Implementace **42**
8.1 Popis platební brány . . . 42
8.2 Postup implementace . . . 46
8.3 Burza Binance a její API . . . 53

8.4 Směnárna Coinbase a její API 61
8.5 Implementace kryptoměn 69
8.6 Technická implementace REST API a jeho popis 76
8.7 Zabezpečení 83

9 Závěr **84**

Literatura **86**

Seznam použitých zkratek a symbolů

API	–	Application Programming Interfacec
ČR	–	Česká Republika
EU	–	Evropská unie
p2p	–	Peer to peer
USD	–	Americký dolar
EUR	–	Euro
LTC	–	Litecoin
BTC	–	Bitcoin
XRP	–	Ripple
ETH	–	Ethereum
DAO	–	Decentralizovaná autonomní organizace
SEPA	–	Single Euro Payments Area
UK	–	United Kingdom
EET	–	Elektronická evidence tržeb
ČNB	–	Česká národní banka
JWT	–	JSON Web Token
UTXO	–	Unspent Transaction Output

Seznam obrázků

1 Bitcoin logo . . . 19
2 Vývoj ceny Bitcoinu 12.listopad 2017 - 12.listopad 2018 . . . 19
3 Vývoj trendu vyhledávání Bitcoinu ve vyhledávači Google [27] . . . 20
4 Litecoin logo . . . 20
5 Vývoj ceny Litecoinu od 25.února 2018 - 25.února 2019 . . . 21
6 Vývoj trendu vyhledávání Litecoinu ve vyhledávači Google [28] . . . 21
7 Ethereum logo . . . 22
8 Vývoj ceny Etherea od 25.února 2018 - 25.února 2019 . . . 23
9 Vývoj trendu vyhledávání Ethereum ve vyhledávači Google [29] . . . 23
10 Ripple logo . . . 24
11 Vývoj ceny Ripple od 25.února 2018 - 25.února 2019 . . . 25
12 Vývoj trendu vyhledávání Ripple ve vyhledávači Google [30] . . . 25
13 Dash logo . . . 26
14 Vývoj ceny Dash od 25.února 2018 - 25.února 2019 . . . 27
15 Vývoj trendu vyhledávání Dash ve vyhledávači Google [31] . . . 27
16 Neo logo . . . 28
17 Vývoj ceny NEO od 25.února 2018 - 25.února 2019 . . . 29
18 Vývoj trendu vyhledávání NEO cryptocurrency ve vyhledávači Google [32] . . . 29
19 Loga platebních bran . . . 37
20 Loga krypto platebních bran . . . 39
21 Zjednodušený proces platby . . . 45
22 Diagram aktivit - Postup ověření transakce . . . 47
23 Diagram aktivit - Postup směny v rámci burzy Binance . . . 50
24 Aplikace - ukázka kurzovního lístku . . . 51
25 Vytvoření API přístupu na burze Binance . . . 53
26 Coinbase - založení API přístupu . . . 61
27 Databázové schéma . . . 76
28 Visual studio - Code map . . . 78

Seznam tabulek

1 Poplatky směnárny Coinbase 48
2 Poplatky burzy Binance 49
3 Použité parametry Binance API - price 54
4 Použité parametry Binance API - GetDepositHistoryAsync 55
5 Použité parametry Binance API - PlaceOrderAsync 56
6 Použité parametry Binance API - QueryOrderAsync 58
7 Použité parametry Binance API - WithdrawAsync 59
8 Použité parametry Coinbase API - GetSellPriceAsync 62
9 Použité parametry Coinbase API - ListDepositsAsync 63
10 Použité parametry Coinbase API - PlaceSellOrderAsync 65
11 Použité parametry Coinbase API - WithdrawalFundsAsync 67
12 API parametry - vytvoření transakce 79
13 API parametry - získání info o transakci 80
14 API parametry - funkce getPrices 81
15 Statické číselníky (Enumerations) 82

Seznam výpisů zdrojového kódu

1 Odpověď Binance API - price . . . 54
2 Binance.NET - GetDepositHistoryAsync . . . 55
3 Odpověď Binance API - GetDepositHistoryAsync . . . 56
4 Binance.NET - PlaceOrderAsync . . . 57
5 Odpověď Binance API - PlaceOrderAsync . . . 57
6 Binance.NET - QueryOrderAsync . . . 58
7 Odpověď Binance API - QueryOrderAsync . . . 59
8 Binance.NET - WithdrawAsync . . . 60
9 Odpověď Binance API - WithdrawAsync . . . 60
10 Coinbase.NET - Inicializace API klienta . . . 62
11 Coinbase.NET - GetSellPriceAsync . . . 62
12 Odpověď Coinbase API - GetSellPriceAsync . . . 63
13 Coinbase.NET - ListDepositsAsync (Litecoin) . . . 63
14 Odpověď Coinbase API - ListDepositsAsync (Litecoin) . . . 64
15 Coinbase.NET - PlaceSellOrderAsync (Litecoin -> EUR) . . . 65
16 Odpověď Coinbase API - PlaceSellOrderAsync (Litecoin -> EUR) . . . 66
17 Coinbase.NET - WithdrawalFundsAsync (EUR) . . . 67
18 Odpověď Coinbase API - WithdrawalFundsAsync (EUR) . . . 68
19 Bitcoin vygenerování nové peněženky . . . 69
20 Odpověď z REST API Chain.so - Zůstatek Bitcoin peněženky [36] . . . 69
21 Odpověď z REST API Chain.so - Získání UTXOS (Bitcoin) . . . 70
22 NBitcoin - vytvoření nové transakce (Bitcoin) . . . 70
23 NBitcoin - vygenerování HEX transakce . . . 71
24 Chain.so - odeslání Bitcoin transakce do sítě . . . 71
25 NBitcoin - Litecoin network . . . 71
26 Nethereum - Vygenerování nové Ethereum peněženky . . . 72
27 Nethereum - Odeslání Etherea do jiné peněženky . . . 72
28 Nethereum - Zjištění zůstatku Ethereum peněženky . . . 72
29 Neo lux - Vygenerování nové NEO peněženky . . . 73
30 Neo lux - Transakce v rámci kryptoměny NEO . . . 73
31 Neo lux - Zjištění zůstatku peněženky NEO . . . 73
32 Node.js - Vygenerování nové Ripple peněženky . . . 74
33 Ripple.NET - Transakce v rámci kryptoměny Ripple . . . 74
34 Ripple API - Zjištění zůstatku peněženky Ripple . . . 75
35 NBitcoin - Dash network . . . 75
36 ASP.NET Core - Automatický dependency injection . . . 77
37 API - odpověď po vytvoření transakce . . . 79

38 API - odpověď funkce getTransactionInfo 80
39 API - odpověď API funkce gerPrices 81

1 Úvod

V roce 2008 vznikla první kryptoměna jménem Bitcoin. Tato kryptoměna měla být první decentralizovaná měna, která umožňuje nezávislost na světových měnách, a stát se jejich alternativou. V následujících letech vznikaly další kryptoměny, které se učily z chyb Bitcoinu a poskytovaly ještě lepší technologická řešení. V té době ještě spousta lidí příliš velkou váhu kryptoměnám nepřisuzovala a v drtivé většině je ignorovali. Jednalo se tudíž o technologii využívanou zcela a pouze nadšenci a znalými lidmi. Běžný uživatel kryptoměny nepotřeboval, protože nebylo možné jimi zaplatit účty, koupit elektroniku či nemovitost.

Postupem času vzrostla cena Bitcoinu, a tak se o kryptoměny začalo zajímat čím dál tím více lidí včetně medií. Media měla v tomto procesu „osvěty“ důležitou úlohu, a právě díky nim se kryptoměny dostaly do povědomí obrovské masy lidí. Tito lidé díky službám jako je například Coinbase měli možnost z displeje svého chytrého mobilního zařízení nakupovat a prodávat kryptoměny v jednotkách minut. Tento nebývalý zájem zapříčinil prudký růst všech kryptoměn.

Vzniklo několik platebních bran, které e-shopy integrovaly, a s velkou pompéznosti oznamovaly, že také přijímají platby pomocí Bitcoinu.

Bez ohledu na pokles cen kryptoměn v roce 2018 jsem se rozhodl v rámci této diplomové práce navrhnout a implementovat vlastní platební bránu, která může fungovat ať už jako řešení platební brány ve vlastním e-shopu nebo jako produkt který je možno poskytovat e-shopům jako externí produkt. Platební brána v rámci této diplomové práce proto nepodporuje pouze kryptoměnu Bitcoin, ale také její mladší sourozence Litecoin, Ethereum, Dash, NEO a Ripple, které mnoho lidí nazývá altcoiny.

V první části diplomové práce shrnu informace o kryptoměnách obecně včetně informací o těchto osmi kryptoměnách, které následně implementuji. Dále popíši, jak kryptoměny získat, jejich bezpečnost, burzy a trhy, které dnes existují, klasické a krypto platební brány nebo legislativu ve vztahu ke kryptoměnám v rámci ČR a EU.

V druhé části se poté zaměřím na implementaci samotné platební brány včetně popisu funkcionality, procesu platby nebo implementace burzy Binance a směnárny Coinbase. Na závěr poté vyhodnotím všechny získané poznatky a navrhnu další možnosti rozšíření v rámci této diplomové práce.

2 Kryptoměny

V posledních několika letech můžeme stále slýchat o tom, jak nám kryptoměny změnily život. Co je to tedy vlastně kryptoměna? A odkud se vůbec vzala?

V roce 2008 neznámý programátor Satoshi Nakamoto (jehož totožnost není do dnešní doby známá) oznámil vznik nové decentralizované měny jménem Bitcoin. Bitcoin který si po rekordním růstu, ale také i po velkém pádu stále drží hodnotu v řádech tisíců dolarů byla úplně první kryptoměna, která vznikla.

2.1 Co je to kryptoměna?

Kryptoměna je decentralizována virtuální měna, kterou lze ve většině případů získat pouze těžením. To znamená že tuto měnu nemá nikdo na starost a nikdo jí neřídí. Dnes si banky drží jednotlivé zůstatky účtů ve svých databázích. V případě že chcete své peníze například odeslat musíte se dotázat do této „centrální“ databáze, zda vůbec máte dostatečné množství peněz. V případě že by byla tato centrální databáze napadena nebo nedostupná můžete k penězům snadno ztratit přístup. A jak to vlastně funguje ve světě kryptoměn? Kryptoměny tím že jsou decentralizovány, tak centrální databázi postrádají a fungují na principu peer to peer sítě. Tato peer to peer síť se skládá z tak zvaných nodů což jsou počítače uživatelů této sítě. Uvnitř této sítě má u sebe každý databázi všech transakcí a stavu účtu každého uživatele Bitcoinu. V případě nové transakce musí tato transakce být podepsána privátním klíčem a je odeslána mezi všechny uživatele v síti. To znamená že každý uživatel si drží aktuální databázi všech transakcí. Toto je v podstatě základní princip p2p sítě. Transakce je téměř okamžitě po odeslání známá všem v dané síti, ale je potřeba ji potvrdit, a to se děje až po nějakém čase. Samotné potvrzení je tedy klíčovým prvkem kryptoměn. Dokud není transakce potvrzena tak je v čekajícím stavu, a tudíž nebyla ještě dokončena. Jakmile je transakce potvrzena vše je hotovo a transakce je přidaná do blockchainu [39] kde zůstane již napořád a není možno ji nijak zrušit nebo změnit. O potvrzení transakcí se starají lidé, kteří těží tzv. mineři (o samotném procesu těžení si povíme něco více v následující kapitole 2.2).[1]

2.2 Jak kryptoměnu získat?

V dnešní době existují tři způsoby, jak kryptoměny získat. První relativně jednoduchým způsobem je nákup. Samotný nákup je nenáročný, když nebereme v úvahu nutnost vlastnit finanční prostředky. Druhým způsobem je bankomat. Těchto bankomatů je po ČR v řádu desítek kusů a je v nich možno nakupovat nebo směňovat kryptoměny. Třetím způsobem je těžba, která je každopádně díky enormnímu rozmachu kryptoměn stále těžší, a vyžaduje obrovský výpočetní výkon.

2.2.1 Těžba

Tím „nejpřirozenějším“ způsobem, jak kryptoměnu získat je tzv. těžba. Těžba je umožněna každému, díky tomu, že decentralizovaná síť nemá žádnou „vyšší autoritu“, která by samotné těžení regulovala. Tvůrce Bitcoinu, Satoshi Nakamoto přišel se způsobem, jak těžbu ztížit, a to tak, že těžaři musí vynaložit na těžbu určitý výpočetní výkon k nalezení hashe, což je produkt kryptografické funkce dané kryptoměny. Tento hash spojuje jednotlivé nové bloky s jeho předchůdci. Takovýto způsob je nazýván anglickým termínem „Proof of work“ a u Bitcoinu je proof of work založen na hashovacím algoritmu SHA 256. Tento hashovací algoritmus je stále v dnešní době velmi bezpečný a je téměř nemožné jej prolomit. Jakmile těžař tento hash získá může pomoci něj ověřit transakci, a tím vytvořit blok v blockchainu [39]. Tímto krokem těžař získá na oplátku určitý počet dané kryptoměny. Vzhledem k obrovskému zájmu o kryptoměny se složitost získání hashe stupňuje, a tím pádem je k těžbě potřeba čím dál tím více výpočetního výkonu. Jelikož se již málo komu oplatí těžit samostatně například Bitcoin, vznikly takzvané mining pooly. Jedná se o skupiny lidí, kteří těží společně, a tím pádem navzájem sdílí výpočetní výkon. V případě, že takováto skupina vygeneruje hash, tak se odměna v podobě kryptoměny rozdělí v určitém poměru mezi členy této skupiny.

Samotná těžba se provádí pomocí grafických karet, které pro vygenerování hashe nabízejí vyšší výkon než CPU. Proto také v roce 2017 nastala krize na trhu grafických karet, jelikož například modely Nvidia GTX 1060, GTX 1070, AMD RX 570 nebo RX 580 začali v obrovském množství nakupovat právě těžaři. Z tohoto důvodu byl nedostatek těchto karet na trhu, jelikož výrobci nestíhali vyrábět nové kusy. V reakci na tuto situaci zareagovali někteří prodejci a prodávali tyto grafické karty pouze za předpokladu, že si zákazník skládal počítačovou sestavu, a tudíž měli danou grafickou kartu k osobním účelům. Nedostatek grafických karet trval do poloviny roku 2018.

2.2.2 Nákup na internetu a bankomaty

Jak již bylo zmíněno v předchozí podkapitole, samotná těžba je u některých kryptoměn pro běžného člověka v podstatě zbytečná. Toto se týká především Bitcoinu u kterého se již dnes těžba jednotlivcům neoplatí.

Dnes existuje mnoho způsobů, jak si kryptoměnu koupit. Tou nejjednodušší cestou je se zaregistrovat, například do služby Coinbase nebo Revolut. V obou dvou případech je po uživateli vyžadováno ověření totožnosti, a to většinou formou vyfocení dokladu a svého obličeje. Následně může zákazník nakupovat kryptoměny za aktuální cenu na trhu. Nicméně, jelikož se jedná o služby, je třeba počítat s jistým poplatkem, který je za danou službu účtován. V případě Revolutu nakupující fyzicky kryptoměnu nevlastní, ale vidí ji pouze ve virtuální formě. Výhodou je například platba kartou, kde je strženo množství dané kryptoměny vůči aktuálnímu kurzu. Naopak v rámci služby Coinbase majitel fyzicky měnu vlastní a může si jí převést do libovolné peněženky. Zkušenější uživatele poté využívají burzy. Každá burza má svůj vlastní trh, v rámci kterého se mohou lišit i ceny jednotlivých kryptoměn mezi těmito burzami. Výhodou oproti výše zmíněným službám jsou menší poplatky a také možnost sledovat aktuální kurz živě. Díky tomu mohou zkušenější uživatelé nakoupit kryptoměny výhodněji.

Poslední možností, jak získat kryptoměnu, je nákup v bankomatu na kryptoměny. Tyto bankomaty se začaly objevovat od 2015 a dostaly se i k nám. V současnosti se nejvíce bankomatů nachází v Praze a následně v Brně a v Ostravě. Výhoda těchto bankomatu neslouží v možnosti zakoupení kryptoměny, ale spíše výběru hotovosti záměnou za určitě množství kryptoměny dle aktuálního kurzu. I v rámci těchto bankomatů je nutno počítat s určitým poplatkem.

2.3 Bitcoin

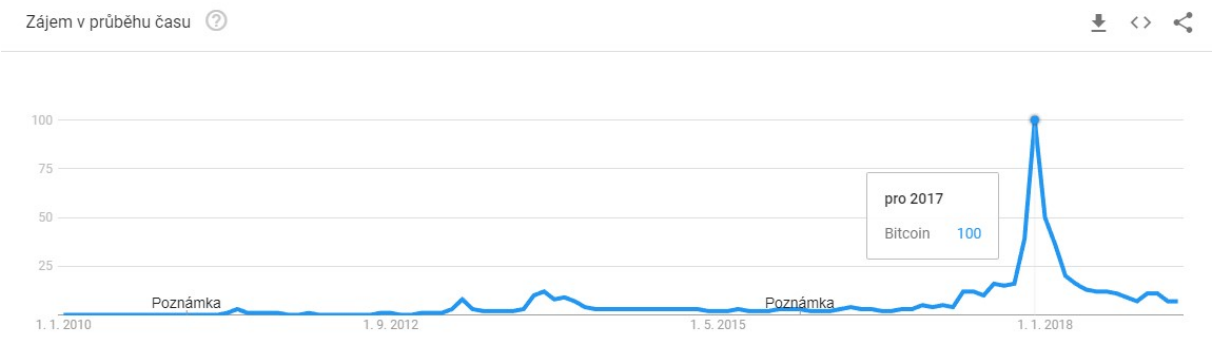
Obrázek 1: Bitcoin logo

Jedná se o první a zároveň nejhodnotnější kryptoměnu na světě. Bitcoin byl v roce 2008 vytvořen neznámým člověkem nebo skupinou s názvem Satoshi Nakamoto. Nakamotova identita je dodnes neznámá. V lednu 2009 byl vytěžen první Bitcoin, a tím vznikl první blok v blockchainu [39], který se nazývá genesis block. Z počátku bylo možné koupit za jeden dolar 1309 Bitcoinů. Postupně jeho cena rostla, až v roce 2017 dosáhl svého vrcholu, a to 19 738 dolarů za jeden Bitcoin. Následně v roce 2018 nastal pád a momentálně se jeden Bitcoin obchoduje přibližně za 5 000 dolarů.

Obrázek 2: Vývoj ceny Bitcoinu 12.listopad 2017 - 12.listopad 2018

Bitcoin splňuje všechny parametry, které kryptoměna má mít. Jedná se tedy o plně decentralizovanou měnu založenou na technologii peer to peer sítě a všechny transakce jsou zaznamenávány do blockchainu [39]. Zároveň je Bitcoin možné těžit a všechny Bitcoin transakce musí být potvrzeny těžaři. Počet Bitcoin bloků je omezen, a jakmile budou všechny bloky vytěženy, nebude již možné Bitcoin těžit. Ačkoliv Bitcoin v posledních měsících výrazně ztratil ze své hod-

noty, tak se stále drží na vrcholu, co se ceny za jednu „minci“ týče. Jeho další vývoj je nicméně nepředvídatelný. [2]



Obrázek 3: Vývoj trendu vyhledávání Bitcoinu ve vyhledávači Google [27]

2.4 Alternativní kryptoměny

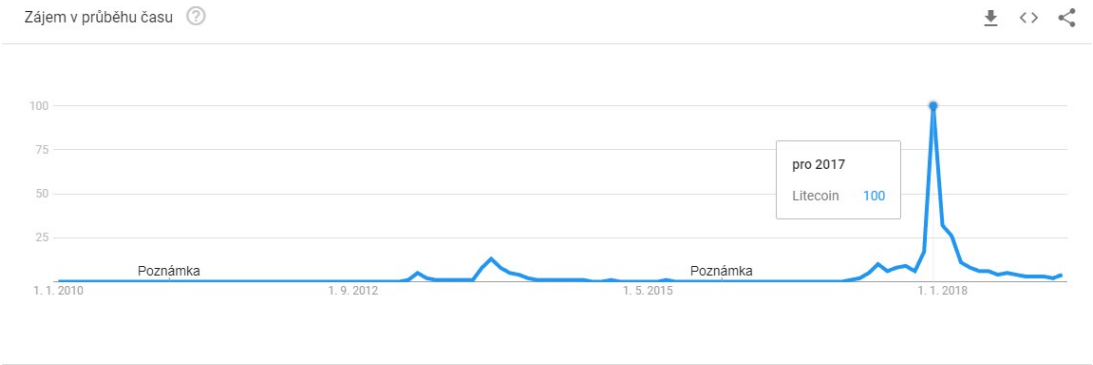
Alternativní kryptoměny nebo někdy také altcoiny, jsou všechny kryptoměny, které vznikly po obrovském úspěchu Bitcoinu. Mnoho těchto altcoinů vzniklo a funguje na podobném principu jako Bitcoin (například Litecoin nebo DASH). Jsou zde ale také altcoiny, které fungují zcela jinak, například Ethereum nebo Ripple. V roce 2018 bylo evidováno něco málo přes 1500 různých altcoinů a další stále vznikají. [3]

2.4.1 Litecoin (LTC)

Obrázek 4: Litecoin logo

Litecoin je první kryptoměna, která vznkla 7.října 2011. Vytvořil jej zaměstnanec Google Charlie Lee, kterému se přezdívá satoshilite (Satoshi je tvůrce Bitcoinu). Z technického hlediska funguje kryptoměna téměř stejně jako Bitcoin. Z počátku byl Litecoin také přezdíván jako stříbrný Bitcoin, protože Bitcoin byl zlatý. Oproti Bitcoinu se liší tím, že čas generování jednoho bloku je 2.5 min (oproti 10 min u Bitcoinu) a počet mincí (coinů) je 4 krát větší než u Bitcoinu. Litecoin je také první kryptoměna, jež využívá hashovací algoritmus scrypt, kdežto Bitcoin využívá hashovací algoritmus SHA256. V lednu 2019 se cena jednoho Liteconu pohybovala něco mezi 27 až 28 € a jeho cena kolísá společně s cenou Bitcoinu. Jeho hodnota je tedy do jisté míry závislá na hodnotě Bitcoinu. Symbol Litecoinu je **Ł** a zkratka **LTC**.

Obrázek 5: Vývoj ceny Litecoinu od 25.února 2018 - 25.února 2019



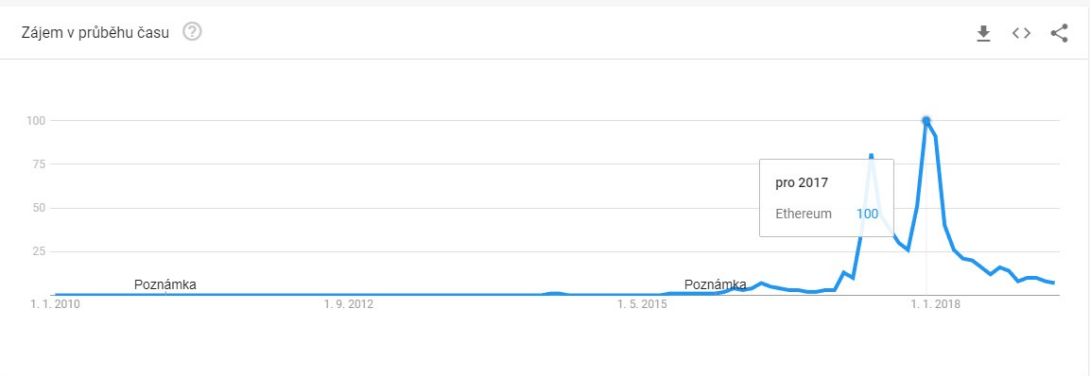
Obrázek 6: Vývoj trendu vyhledávání Litecoinu ve vyhledávači Google [28]

2.4.2 Ethereum (ETH)

Obrázek 7: Ethereum logo

Ethereum je další velmi známou alternativní kryptoměnou. Jedná se o open source softwarovou platformu založenou na technologii blockchainu [39]. Zároveň je to také decentralizovaný kompletní turingovský virtuální stroj, který se nazývá EVM (Ethereum Virtual Machine). Tento virtuální stroj umožňuje běh takzvaných Smart kontraktů. Tyto kontrakty zajišťují hladké a nezmanipulovatelné fungování Ethereum sítě. Platforma také umožňuje vývojářům vytvářet decentralizované aplikace. Ethereum bylo nejprve vymyšleno ke konci roku 2013 Vitalikem Buterinem, a následně vyvinuto v roce 2015 díky crowdfundingu, který vývoj zaplatil. V roce 2016 byla kvůli krádeži měny v hodnotě 50 milionů dolarů měna rozdělena na Ethereum a Ethereum classic. V Ethereu byla tato krádež vzata zpět a Ethereum classic pokračuje nadále v původním stavu (tedy včetně krádeže). Každá transakce je zpoplatněna a jako poplatek za transakci je využívána jednotka GAS. Stejně jako Bitcoin, je Ethereum veřejná distribuována blockchain [39] síť. Nicméně Bitcoin je striktně určen k online platbám, kdežto Ethereum blockchain je zaměřen na to, aby v něm mohla běžet jakákoliv decentralizovaná aplikace.

Obrázek 8: Vývoj ceny Etherea od 25.února 2018 - 25.února 2019



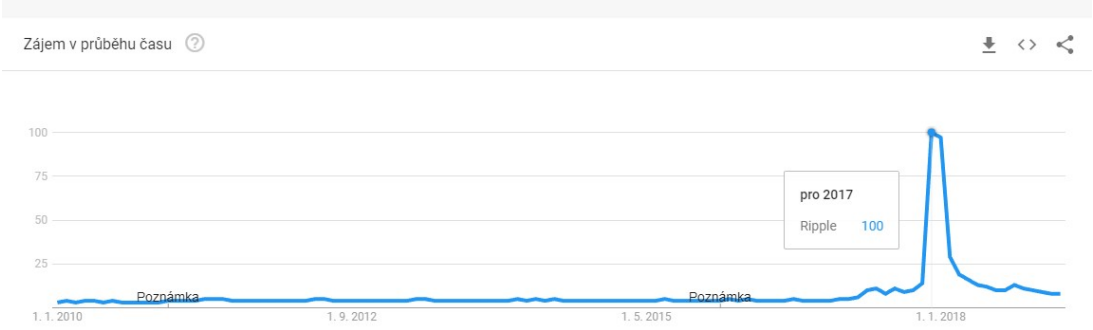
Obrázek 9: Vývoj trendu vyhledávání Ethereum ve vyhledávači Google [29]

2.4.3 Ripple (XRP)

Obrázek 10: Ripple logo

Ripple je celosvětová platební síť, ve které se používá kryptoměna XRP (Ripple). Tato síť vznikla v roce 2012, a to s cílem eliminovat poplatky za transakce a směnu. Zároveň také eliminuje časovou prodlevu mezi odesláním a přijetím platby. Oproti Bitcoinu a jiným kryptoměnam se ale nejedná úplně o sto procentní kryptoměnu. Tato kryptoměna se oproti ostatním liší tím, že ji kontroluje jedna firma, a tím v podstatě podkopává princip decentralizace. Zároveň kryptoměna nevzniká formou Proof of work (tzn. netěží se). Sto procent této kryptoměny je tzv. pre-mined, a to znamená, že ji není potřeba těžit. Více než 60% této kryptoměny drží majitel Ripple labs. Z tohoto důvodu tato kryptoměna není úplně nezávislá. Každopádně je potřeba zmínit, že těchto 60% je uzamčeno pomocí časového zámku, což znamená, že toto množství kryptoměny není okamžitě k dispozici, ale je majiteli postupně uvolňováno v daném množství za daný čas. To zabrání tomu, aby byl trh v jednom momentě zaplaven velkým množstvím této kryptoměny. I přes tyto nedostatky se stále jedná o jednu z momentálně nejúspěšnějších kryptoměn.[4]

Obrázek 11: Vývoj ceny Ripple od 25.února 2018 - 25.února 2019



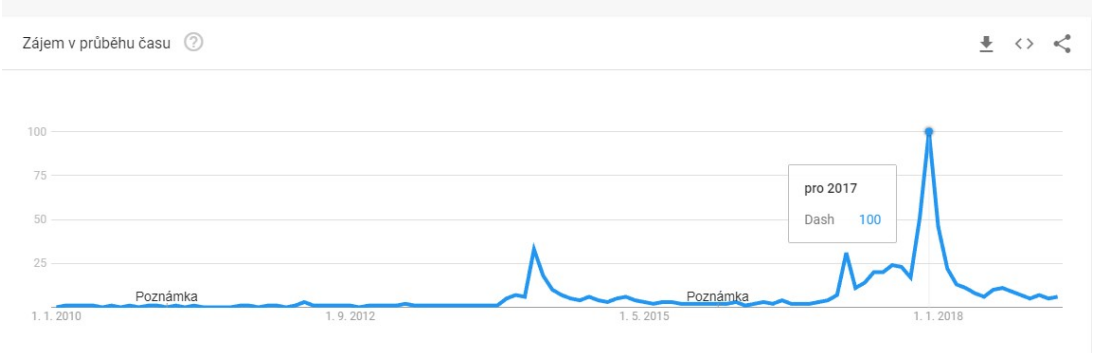
Obrázek 12: Vývoj trendu vyhledávání Ripple ve vyhledávači Google [30]

2.4.4 Dash

Obrázek 13: Dash logo

Dash (kdysi také Darkcoin nebo XCoin) je decentralizovaná kryptoměna, která umožňuje soukromé a okamžité transakce. Jedná se o DAO (decentralizovanou autonomní organizaci), kterou řídí tzv. masternodes. Zároveň je těžení rozděleno tak, že 45% vytěžených coinů putuje těžařům, dalších 45% vytěžených coinů putuje masternodům a zbylých 10% vytěžených coinů putuje do fondu do kterého DAO investuje. Dash je založen na protokolu Bitcoinu. Kryptoměna byla spuštěna v lednu roku 2014 Evanem Duffieldem. K těžbě se využívá hashovací algoritmus X11 a k vytěžení jednoho bloku dochází cca každé dvě a půl minuty. Ačkoliv se díky masternodům může zdát, že jde stejně jako v případě Ripple porušován princip decentralizace, tak tomu tak úplně není. Tyto obavy totiž vyvrací možnost navrhnout vlastní inovaci v rámci kryptoměny. Za každý takovýto návrh uživatel zaplatí 5 mincí DASH. V případě, že jeho návrh uspěje obdrží navrhovatel mince z tzv. super blocku, v kterém se po dobu 30 dní hromadí 10% všech vytěžených mincí. O tom, kdo tyto mince obdrží, rozhodují masternodes, a to v transparentním hlasování. V lednu 2019 se cena za 1 DASH pohybovala okolo 58 €. [5]

Obrázek 14: Vývoj ceny Dash od 25.února 2018 - 25.února 2019



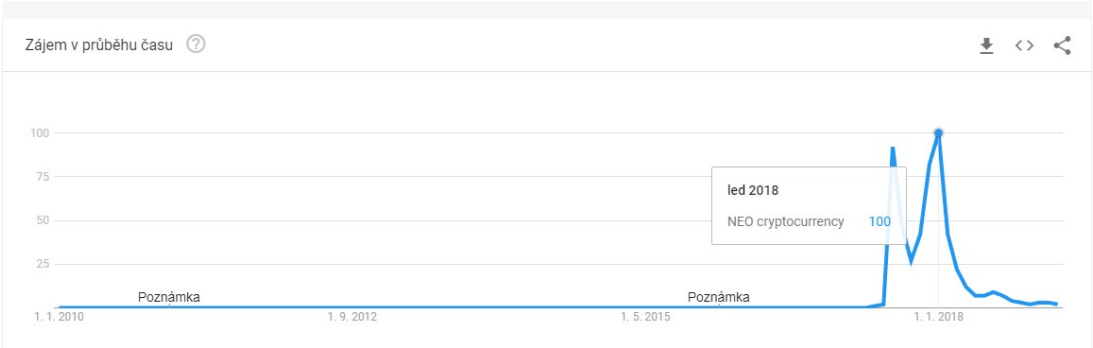
Obrázek 15: Vývoj trendu vyhledávání Dash ve vyhledávači Google [31]

2.4.5 Neo

Obrázek 16: Neo logo

V roce 2014 vzniklo NEO pod jménem AntShares, který byl založen v roce 2014 Da Hongfeiem a Erikem Zhangem. Jednalo se o první čínskou blockhain platformu. V roce 2017 byl AntShare přejmenován na Neo. Jelikož se jedná o čínskou kryptoměnu, může mít čínská regulace dopad na cenu této kryptoměny. Neo funguje na podobném principu jako Ethereum, ale vzhledem k tomu, že vzniklo později, poučilo se z jeho nedostatků. Proto se mu také někdy přezdívá čínské Ethereum nebo dokonce Ethereum killer. Stejně jako u Etherea je jako poplatek za transakce využívána jednotka GAS.

Obrázek 17: Vývoj ceny NEO od 25.února 2018 - 25.února 2019



Obrázek 18: Vývoj trendu vyhledávání NEO cryptocurrency ve vyhledávači Google [32]

3 Bezpečnost

Vzhledem k rychlému nástupu kryptoměn a obrovskému počtu lidí, kteří do nich rapidně investují, také vzrostlo riziko krádeže. Jsou zde samozřejmě případy jak krádeží, tak nechtěných ztrát větších částek kryptoměn. Tato kapitola se zaměří na bezpečnost a anonymitu kryptoměn, ale také na rizika a způsoby, jak se těmto rizikům vyhnout. Kryptoměny s sebou přináší mnoho rizik, jelikož reprezentují velké množství peněz.

3.1 Jsou kryptoměny bezpečné?

V rámci kryptoměn je krádeží myšlen nedovolený vstup do peněženky uživatele a odeslání kryptoměny na cizí účet. Tyto krádeže se mohou provést několika způsoby, jako je například phising, scamming nebo hacking. V krajních případech je možné také ukrást kryptoměnu, která není uložena na počítači připojeném k síti. Nicméně v takovém případě se nejedná o kybernetický útok, nýbrž fyzický.

Dle statistik [6] byly v první polovině roku 2018 ukradeny kryptoměny v hodnotě přesahující 1.1 miliardy amerických dolarů. Vzhledem k této informaci je ještě více zajímavější to, že více než 56% [7] těchto krádeží se děje ve Spojených státech.

Jak už bylo zmíněno, většina z těchto útoků se děje virtuální cestou a jeden z nejznámějších útoků byl proveden mezi lety 2011 až 2014 na Japonskou burzu Mt. Gox, při kterém byly ukradeny Bitcoiny v celkové ceně 350 milionů amerických dolarů. Jednalo se o první krádež takovéhoto měřítka. Tento útok následně ve většině lidí, kteří do kryptoměn investovali vyvolal otázku, zdali jsou jejich investice v bezpečí. Tento incident měl také pozitivní dopad, jelikož zabezpečení burz od té doby zesílilo.

Nejznámější útoky [9]:

- **Bitstamp** – V roce 2015 byly odcizeny kryptoměny v hodnotě 5 milionů dolarů
- **Mt. Gox** – Mezi lety 2011 a 2014 byly odcizeny Bitcoiny v hodnotě 350 milionů dolarů.
- **Bitfinex** – V roce 2016 byly odcizeny kryptoměny v hodnotě 72 milionů dolarů. Uživatelům byly kryptoměny vráceny.
- **NiceHash** – V roce 2017 byly odcizeny kryptoměny v hodnotě 60 milionů dolarů.
- **Coincheck** – V roce 2018 byla odcizena kryptoměna NEM v hodnotě 400 milionů dolarů.
- **Zaif** – V roce 2018 bylo odcizeno 60 milionů dolarů v kryptoměnách Bitcoin, Bitcoin cash a Monacoin.

Samotné kryptoměny jsou ve svém základu bezpečné. To znamená, že každý uživatel má svou peněženku a k této peněžence vlastní klíč. Tento klíč uživateli dovoluje posílat kryptoměny z peněženky pryč, což znamená, že je vlastníkem. Tento způsob je tedy relativně jasný a bezpečný. Na druhou stranu záleží na každém uživateli, jak si tento klíč chrání a kde jej uchovává. Drtivé množství všech útoků a krádeží totiž nebyl na zabezpečení kryptoměn samotných, ale využití bezpečnostních děr typu Heartbleed nebo Padding Oracles. To znamená, že útočník nevyužil bezpečnostní chybu kryptoměny, ale protokolů, které využíval počítač obsahující klíč k peněžence. Následně po proniknutí do počítače nebylo nic jednoduššího, než ukrást klíč od peněženky a převést celý obsah peněženky na svou peněženku. Jakmile toto útočník provedl, tak díky využití technologie blockchain [39] není možno tuto transakci už nijak zvrátit, a proto bylo dané množství kryptoměny navždy ztraceno. Technologie kryptoměn je tedy sama o sobě bezpečná. Nebezpečí si vytvářejí sami uživatelé, když své klíče k peněženkám ukládají na místech, která mohou být napadena, nebo mají bezpečnostní díry. [8]

3.2 Jak se chránit?

Jak už bylo řečeno, jediný způsob, jak útočník může vaše kryptoměny odcizit, je zjištění vašeho klíče k peněžence. Zde je seznam kroků, které by měl každý kdo vlastní kryptoměny dodržovat.

1. Vybrat kvalitní peněženku, která zároveň nějakým způsobem šifruje klíč k peněžence například heslem
2. Využívat dvou faktorové přihlášení jak na burzy, tak k e-mailovému klientovi. Dvou faktorové ověření je například SMS kód potřebný k přihlášení.
3. Vygenerovat si všude silná hesla a uložit si je například do 1Passwordu
4. Používat kvalitní antivirový software např. ESET, Avast apod.
5. Mít kryptoměny rozmístěné po menších částkách mezi více peněženek
6. Sdělit přístupová hesla nejbližší rodině v případě, kdyby se něco stalo. V opačném případě by mohlo být jmění uložené v kryptoměnách navždy ztraceno.

V případě větších služeb, které mají ve správě velké množství peněženek (například burzy), je ochrana složitější. Především je potřeba mít ještě navíc k předchozím krokům zabezpečené servery, na kterých jsou klíče od peněženek uloženy. To znamená mít vyřešeny všechny známé bezpečnostní chyby typu Heartbleed nebo Padding Oracles.

V žádném případě se tyto bezpečnostní pravidla nesmí podcenit, jelikož v opačném případě získává útočník šanci ke krádeži.[10]

3.3 Anonymita

Anonymitou je myšleno to, že neexistuje záznam o identitě (adresa, jméno, číslo účtu) majitele kryptoměny. Samotné transakce jsou již ze své podstaty (blockchain [39]) veřejné, a proto jediným způsobem, jak zůstat v anonymitě, je nespojit svou osobu s konkrétní peněženkou. Jednou z velkých výhod kryptoměn je ta, že si uživatelé mohou vytvářet nekonečný počet nových peněženek, a tím svou anonymitu zvyšovat.

I přes to vše je v dnešní době možné spojit konkrétní osobu s peněženkou. Jeden ze způsobu je například analýza útrat. V případě, že si uživatel zakoupí pomocí kryptoměn nějaké zboží v e-shopu, a zadá dodací adresu včetně jména a příjmení. Tak na základě tohoto nákupu okamžitě existuje záznam o tom, kdo platbu provedl, a díky tomu je možno spojit tyto údaje s peněženkou. Dalším způsobem je také IP adresa, která je při transakci zaznamenána. Zkušenější hackeři můžou poté podle IP adresy dohledat majitele peněženek.

V případě, že uživatel chce opravdu zůstat anonymní, jsou zde kryptoměny, které to umožňují. Jedná se o kryptoměnu DASH, která poskytuje možnost provést anonymní transakci pomocí funkce, která se nazývá PrivateSend. Tato funkce vmísí transakci mezi několik jiných transakcí tak, aby ji nebylo možno dohledat.

Anonymita je tedy v rámci kryptoměn opravdu relativní pojem. V základu každá kryptoměna poskytuje určitou úroveň anonymity a záleží poté na každém z uživatelů, jak tuto anonymitu zvýší nebo naopak sníží.[11]

4 Burzy a trh

Vzhledem k vysoké popularitě kryptoměn v posledních letech vzniklo nespočet burz, které umožňují jak nákup, tak prodej širokého spektra kryptoměn. V samotném počátku kryptoměny Bitcoin nebylo pro běžného uživatele vůbec jednoduché tuto kryptoměnu získat, případně vyměnit například za měnu reálnou. Dnes je tomu přesně naopak. Burz mezi lety 2015-2019 vzniklo obrovské množství, a proto je možné jakoukoliv kryptoměnu koupit nebo prodat. Z tohoto důvodu začali do kryptoměn investovat rovněž laici, kteří si od investice slibují rychlý zisk. V návaznosti na to také v roce 2017 Bitcoin zaznamenal největší růst v historii, po kterém dle očekávání nastal rychlý pád. Tyto burzy zároveň dohromady tvoří trh, a ačkoliv se cena konkrétní kryptoměny může burzu od burzy lišit, tak jsou to právě burzy, které určují cenu kryptoměn.

Vzhledem k nutnosti verifikace identity u drtivé většiny těchto burz dochází k jisté deanonymizaci. To znamená, že v době nákupu anebo případného prodeje kryptoměn už není člověk anonymní, a je velmi snadné ho v krajním případě také dohledat. Tyto údaje nejsou veřejné a přístup k nim má pouze správce burzy, popřípadě úřady s potřebným povolením.

4.1 Burzy kryptoměn

Jak už bylo zmíněno, burz, které se zabývají pouze kryptoměnami, v poslední době vzniklo nespočet. Bude následovat výčet těch nejznámějších a jejich princip fungování. Mezi TOP 10 burz s kryptoměnami patří tyto [12] :

- **Coinbase**
- **Binance**
- **Kraken**
- **Coinmama**
- **Bitpanda**
- **CEX IO**
- **Bitstamp**
- **Gemini**
- **Changelly**
- **Bitfinex**

Jedná se pouze o stručný výčet vzhledem k množství těchto burz. Většina těchto burz funguje na velmi podobném principu jako například burzy měnové. Trh určují samotní prodejci a nákupčí, a dle objemu nákupů cena kryptoměny klesá nebo stoupá. Všechny tyto burzy také nabízejí kromě Bitcoinu širokou škálu různých kryptoměn, se kterými může být obchodováno.

Prvním krokem k tomu, aby člověk mohl kryptoměny prodávat nebo nakupovat, je nutnost registrace. V rámci této registrace je následně potřeba vyplnit všechny základní údaje, jako je například jméno, příjmení, adresa nebo email. Tyto údaje musí být pravdivé, jelikož drtivá většina z těchto burz vyžaduje takzvané ověření identity. Ověření identity spočívá v tom, že uživatel musí naskenovat svůj doklad totožnosti. Tímto dokladem totožnosti je myšlen například občanský průkaz, řidičský průkaz nebo cestovní pas. V případě některých burz je možné se setkat také s dvojitou kontrolou, a to tak, že je vyžadováno nahrání oboustranně minimálně dvou odlišných dokladů. Zároveň je také možné setkat s tím, že je po uživateli vyžadováno pořízení fotografie v reálném čase. Není tedy možno nahrát například statickou fotografii, ale je ji nutno pořídit pomocí webkamery nebo mobilního zařízeni v daný moment. A k čemu tedy vlastně jsou takto silná bezpečnostní opatření? Jedná se o eliminaci uživatelů, kteří by se pokusili prát špinavé peníze skrze tyto burzy nebo by svým jednáním páchali trestnou činnost.

Když bych chtěl zmínit jednu burzu (směnárnu) která se něčím liší nebo tedy alespoň lišila v minulosti, tak by to byl Coinbase. Momentálně se jedná o jednu z největších burz (směnáren), která existuje. Podařilo se jim prosadit díky jednoduchosti v podobě mobilní aplikace. Není totiž nic jednoduššího než si stáhnout aplikaci Coinbase do svého chytrého mobilního zařízení, zaregistrovat se, vložit svou kreditní kartu a nakupovat kryptoměny. Samozřejmě že většina výše zmíněných burz to v dnešní době také umožňuje, ale kouzlo Coinbase bylo v tom že byli jedni z prvních, kteří tento způsob nakupování kryptoměn protlačili mezi masu lidí, kteří do té doby o kryptoměnách nic nevěděli. Velice rychle se tedy ze začínající firmy stala miliardová společnost, a z majitelů udělala miliardáře. Jedná se tedy o zářný příklad toho, jak zbohatnout na kryptoměnách bez toho, aniž by do nich člověk investoval, jelikož tato firma zbohatla hlavně díky množství transakcí a poplatku z nich. Poplatky mají všechny krypto burzy bez výjimky. Jedná se o způsob obživy těchto krypto burz. Nicméně o samotných poplatcích a omezeních těchto burz si něco řekneme v následující kapitole.

Burzy tedy jsou, a i nadále budou jedním z hlavních míst, kde lidé mohou kryptoměny nakupovat a zároveň je prodávat. Také se jedná o jisté bezpečnostní riziko, a to v případě, že jsou kryptoměny na těchto burzách skladovány. Je totiž jistá pravděpodobnost, že někdy dojde k nějakému hackerskému útoku, který může majitele o tyto kryptoměny připravit. Doporučuje se tedy uchovávat své kryptoměny na více místech (hlavně u sebe) a na burzách mít jen potřebné množství, s kterým chci obchodovat.

4.2 Poplatky a omezení

Každá kryptoměnová burza má nastavený svůj poplatkový systém. Může se jednat jak o fixní částku v rámci transakce, tak o procentuální částku z celkového objemu transakce. V případě

směny kryptoměn na reálnou měnu jsou zde také poplatky například za SEPA převod. Zkrátka většina úkonů, který vydělá nám tak vydělá také burze. Podobně to například funguje u většiny bank, které si rovněž za své služby účtují poplatky. Vypsány budou poplatky v rámci deseti burz, které již byly zmíněny:

- **Coinbase** - Poplatky za nákup/prodej fixní od 0.99$ do 2.99$ u maximálního objemu transakce 200$. Vyšší objem transakce 1.49% z celkové částky. Nákup pomocí kreditní karty 3.99% z částky. [14]
- **Binance** - Poplatek u každé transakce 0.1% a s objemem transakcí se poplatek může snížit až na hodnotu 0.02% podle měsíčního objemu transakcí. Vybrat je možno pouze kryptoměny, a to odesláním na peněženku. U každé kryptoměny je poplatek za výběr jiný a zároveň je potřeba vybrat určené minimální množství. Směna za reálnou měnu není možná. [13]
- **Kraken** - Poplatek je zde jak pro nakupujícího tak pro prodávajícího. Opět stejně jako u Binance jsou zde poplatky na základě objemu transakcí za 1 měsíc. Poplatky začínají na 0.16 % pro prodávajícího a 0.26% pro kupujicího a mohou se dostat až na 0% pro prodávajícího a 0.10% pro kupujicího. [15]
- **Coinmama** - 5% poplatek za použití kreditní karty + 5,9 % z každé transakce. [16]
- **Bitpanda** - 1,49% za nákup Bitcoinu a 1,29% za prodej Bitcoinu. [17]
- **CEX IO** - Poplatek je určen na základě měsíčního objemu transakcí. Poplatek se může pohybovat od 0,25% za nákup a 0,16% za prodej do 0,10% za nákup a 0% za prodej. Zároveň je zde poplatek za vklad pomocí kreditní karty 2,99% a za výběr v případě EUR 1.2% + 5 €. [18]
- **Bitstamp** - Poplatek je zde určen na základě měsíčního objemu transakcí, a to v rozsahu od 0,25% do 0,10%. Zároveň je zde poplatek za použití kreditní karty o velikosti 5% z celkové částky.
- **Gemini** - V případě této burzy jsou zde opět poplatky určovány na základě měsíčního objemu transakcí. Poplatek se pohybuje od 1% do 0% z celkové hodnoty transakce. [21]
- **Changelly** - Changelly si účtuje pouze 0,5% poplatek z celé částky, každopádně vzhledem k slabším směnným kurzům jsou zde skryté poplatky započítány přímo do kurzu. [20]
- **Bitfinex** - Poplatky za nákup jsou zde opět určovány dle měsíčního objemu transakcí. Velikost poplatku se pohybuje od 0.1% za prodej a 0,2 % za nákup do 0% za prodej a 0,055% za nákup. Dále jsou zde poplatky za výběr a vklad kryptoměn a t například v případu Bitcoinu 0,0004 BTC za vklad i výběr. [22]

4.3 Trh s kryptoměnami

Trh s kryptoměnami za posledních několik let raketově vystřelil a zároveň zaznamenal nemalý pád. Každá kryptoměna má svůj vlastní trh a popsán bude ten úplně první, a to Bitcoin. Bitcoin, jak už bylo řečeno, byla první kryptoměna, a proto se tedy jednalo o první trh s kryptoměnou, který vznikl. Samotný trh tvoří běžní uživatelé, investoři nebo burzy. Tento trh poté určuje cenu samotného Bitcoinu. Je to z toho důvodu, že se jedná se princip kryptoměn. Bitcoin ve svém počátku neměl téměř žádnou cenu a jednalo se spíše o zajímavou technologii. Postupem času ale jak uživatele, tak investoři pochopili důležitost této technologie a začali pomalu tuto kryptoměnu nakupovat. To zapříčinilo, že více a více lidí začalo tuto kryptoměnu těžit tak, aby byl na trhu dostatek mincí, vzhledem jejich omezenému počtu. Díky tomu cena Bitcoinu rostla. Největší růst zaznamenala až se vstupem tzv. amatérských investorů, kteří na trh vstoupili s vidinou rychlého zisku, a kteří začali nakupovat kryptoměny ve velkém množství. To zapříčinilo rekordní růst cen všech kryptoměn a nejvíc již zmíněného Bitcoinu. Jedná se o princip poptávky a nabídky. V případě, že by o kryptoměnu nebyl zájem, cena by s velkou pravděpodobností klesala, ale díky velkému zájmu světových medií, tento zájem byl obrovský, díky čemuž cena rostla. Neexistuje zde tedy žádná vyšší autorita, která určuje cenu kryptoměny na trhu.

Samozřejmě jsou zde i vnější vlivy, které mohou mít na cenu kryptoměny vliv. Například v případě Litecoinu to ve většině případů byl tvůrce Litecoinu, který často na svém Twitteru oznamoval například vylepšení technologie. V případě kladné zprávy trh reagoval pozitivně a cena rostla, zatímco v případě špatné zprávy trh okamžitě reagoval poklesem. Je tedy zřejmé, že na cenu kryptoměny mohou mít vliv například technické změny. Dalším příkladem je referendum o Brexitu. Když si obyvatele UK odhlasovali Brexit tak Libra raketovým tempem padala, ale Bitcoin naopak rostl. Je to z toho důvodu, že Bitcoin je nezávislý, a tudíž odolnější vůči událostem jakéhokoliv státu.

Stáleje zde obrovské riziko krachu. V případě, že by například zkrachoval trh s Bitcoinem, dá se očekávat, že by s sebou stáhl většinu kryptoměn a otázkou je, jestli by nějaká přežila. Je pravda, že toto riziko je nepravděpodobné, ale stejně jako globální ekonomická krize, i tato varianta může nastat, a je třeba s ní počítat. I z tohoto důvodu kryptoměnám někteří lidé stále nevěří a nazývají trh s kryptoměnami pouze bublinou, která jednou praskne. Častým kritikem je například americký miliardář a investor Warren Buffet, který kryptoměny nazývá zlem.

Trh s kryptoměnami je obrovský a pohybuje se v něm obrovské množství peněz. V současné době to s trhem nevypadá nejlépe. Kryptoměny si po velkém pádu v roce 2018 stále drží relativně vysokou cenu. Jak již bylo zmíněno, cena je určena trhem, který je ovlivněn mnoha faktory. V případě kryptoměn je tedy doporučeno investovat obezřetně a nesázet na ně celé své jmění a úspory. Zároveň se ale jedná o legitimní způsob, jak zbohatnout.[23]

5 Klasické platební brány

Obrázek 19: Loga platebních bran

Vzhledem k rychlému rozvoji internetu je dnes také platba online jednou z jeho nedomyslitelných funkcí. Platba online nám umožňuje okamžitě zaplatit jakékoliv zboží, které jsme si zakoupili kdekoliv na světě. K tomu, aby prodejce mohl přijímat platby online, musí podporovat nějakou z platebních bran. Tato kapitola se bude zabývat jednou z nejpoužívanějších platebních bran v ČR GoPay a nejpoužívanější světovou platební branou PayPal.

5.1 GoPay

GoPay je česká platební služba, která nabízí obchodníkovi 29 platebních metod v rámci České republiky. Zároveň také kromě platebních metod určených pro ČR poskytuje platební metody pro Slovensko, Chorvatsko, Polsko, Maďarsko, Rumunsko a Bulharsko. Díky tomuto portfoliu se jedná o službu v dnešní době hojně využívanou. Služba je určena pro široké spektrum obchodníků, ať už pro e-shopy s fyzickým nebo digitálním obsahem, tak i pro služby, které vyžadují předplatné, tzn. opakované platby.

Samotná brána pro zákazníka funguje velice jednoduše. V rámci nákupu existují dva typy platby a to tzv. inline nebo redirect platba. Inline platba je typ platby, kde při potvrzení objednávky vyskočí platební okno služby GoPay přímo na stránce obchodníka. Jedná se tedy o jakési překrytí. V případě redirect platby, jak už název napovídá, se jedná o přesměrování zákazníka na web GoPay, kde bude následně vyzván k vyplnění platebních údajů a potvrzení platby. Podle průzkumu firmy GoPay při využití inline platby dokončí platbu o 9,3% zákazníku více. Výhodou je také možnost si bránu nastylovat do firemních barev včetně využití loga firmy. V případě, že e-shop cílí na zahraniční klienty, podporuje GoPay několik světových jazyků, jako například polštinu, angličtinu a podobně. Brána také umožňuje rekapitulaci košíku tak, aby zákazník měl přehled o tom, za co platí. GoPay plně podporuje EET, každopádně od 1.3.2018 se EET netýká obchodníků, kteří nemají kamenný obchod. V případě, že pro obchodníka tato výjimka neplatí, může si při každé platbě nechat vygenerovat EET účtenku, která bude spolu s potvrzením o platbě zaslána přímo zákazníkovi. V případě, že by zákazník nebyl se zbožím nebo službou spokojen, je zde také možnost storna platby a vrácení peněz zákazníkovi přímo na účet.

5.2 PayPal

Tato brána umožňuje přesuny peněz mezi jednotlivými účty v rámci PayPal. Tyto účty jsou poté identifikovány pomocí e-mailové adresy. Každý účet má k sobě připojenou jednu nebo více platebních karet. Tyto platební karty musí mít samozřejmě povolené platby na internetu. Po samotném připojení platební karty není potřeba v rámci platby nic řešit. Stačí se pouze přihlásit a platbu potvrdit bez nutnosti zadávat PIN nebo SMS potvrzení. Největší rozmach zažil PayPal několik let dozadu, kdy neexistovala žádná alternativa. Paypal na rozdíl od obyčejného převodu z účtu na účet provedl platbu okamžitě a klient mohl tudíž například získat digitální kopii hry okamžitě. Před deseti lety neměl PayPal konkurenci a byl podporován většinou e-shopů. Vznikl díky jednomu z největších vizionářů současnosti, Elon Musk, který jeho prodejem společnosti eBay získal 165 milionu dolarů.

V praxi se jedná o velice podobný způsob, jako má GoPay, který se pravděpodobně inspiroval právě u PayPalu. Jelikož je PayPal sám o sobě platební metodou, nenabízí více platebních metod jako například služba GoPay. Je proto možno platit pouze pomocí PayPal účtu, popřípadě pokud zákazník účet nemá, může zaplatit pomocí platební karty. Samotný platební proces je proto velice jednoduchý. V praxi to znamená, že se zákazník po přesměrování na PayPal pouze přihlásí, zkontroluje platební údaje a platbu potvrdí.

6 Krypto platební brány

Obrázek 20: Loga krypto platebních bran

Jak už bylo zmíněno v předchozích kapitolách, kryptoměny jsou dnes na vzestupu, a nejedná se pouze o měnu na investice, ale také pro placení. Samotný princip kryptoměn není úplně nejjednodušší, a proto zde za poslední roky vzniklo několik platebních bran, které poskytují obchodníkovi jednoduchý způsob, jak přijímat platby, například v Bitcoinech.

Jelikož je nyní trh s kryptoměnami obrovský, tak zde za poslední roky vzniklo několik takovýchto platebních bran. Většina platebních bran funguje na stejném principu, proto nebudou uvedeny všechny. Princip platby je tedy stejný jako v případě běžné platby platební kartou. Rozdíl je jediný, a to že kryptoměna je posílána z krypto peněženky. Například u platební brány BitcoinPay je princip následující. Uživatel stiskne tlačítko pro platbu kryptoměnou. Následně je přesměrován na stránku BitcoinPay, kde je zobrazen postup platby včetně adresy peněženky, na kterou má uživatel platbu zaslat. Oproti platbě platební kartou je ale tato transakce o dost pomalejší, jelikož po zaslání kryptoměny je potřeba počkat na potvrzení platby, a to například v rámci kryptoměny Bitcoin může trvat i 30 min (většinou ale do 20 minut). V Česku platbu kryptoměnami podporuje několik e-shopů včetně toho největšího Alza.cz, každopádně díky postupnému úpadku kryptoměn tyto e-shopy ubývají. Vzhledem k tomu, že ceny kryptoměn kolísají, je přijímání plateb pomocí kryptoměn pro e-shopy rizikové, a ne každý z nich je ochotný toto riziko podstoupit. V Česku je velice rozšířena platební brána BitcoinPay, kterou vymysleli a vlastní ji Češi. Ze zahraničních platebních bran zde například mohu zmínit Coinpayments nebo Coingate. Další z nevýhod využití těchto platebních bran je ta, že stejně jako u klasických platebních bran i zde si poskytovatel platební brány bere určitý procentuální poplatek. Tento poplatek mají všichni a vyhnout se mu dá jen v případě, že se e-shop rozhodne implementovat svou vlastní platební bránu.

Časem tedy uvidíme, zda krypto platební brány budou stále více součástí platebních možnosti v košících e-shopů, nebo se jedná pouze o jistý trend v rámci kryptoměn. V průběhu let by však každý e-shop měl mít možnost platby kryptoměnami, stejně tak jako platba kartou.

7 Legislativní rámec ve vztahu ke kryptoměnám

Jak je dobře známo většina úřadů nepracuje příliš rychle. Vzhledem k rychlému nástupu kryptoměn tedy většina států na tento fenomén nijak nereagovala. Tato kapitola se zaměří na vnímání kryptoměn v rámci zákonů České republiky a Evropské unie. Kryptoměna není hotovost, jelikož nemá žádnou fyzickou podobu. Každopádně kryptoměna se v dnešní době dá velice jednoduše vyměnit za hotovost. Některé vlády považuje kryptoměny za určitou hrozbu vůči tradiční měně a snaží se kryptoměny jakýmsi způsobem regulovat nebo i v nejhorším případě omezit.

7.1 V České Republice

V České republice je Česká národní banka (ČNB) centrálním orgánem, který dohlíží nad finančním trhem v zemi. Dle jejich názoru z roku 2015 kryptoměny nejsou peněžní prostředky a ani elektronické peníze. Nákup ani prodej tedy nepředstavuje žádnou platební službu. Kryptoměny nemají ani povahu cenných papírů.

To vše znamená, že v České republice neexistuje ze strany státu žádná regulace a ani žádná zvláštní úprava v daňovém právu. Do roku 2017 byly kryptoměny a operace s nimi mimo národní legislativní regulaci. Dodržovala se pouze závazná legislativní norma EU díky rozhodnutí soudního dvoru EU. Rozhodnutí bylo takové, že Bitcoinové transakce jsou osvobozeny od DPH. Vzhledem k tomu, že jsme členy EU, musela se Česka republika tímto nařízením řídit. Většina členů EU se tímto rozhodnutím tedy řídila až na Polsko, které v důsledku rozhodnutí jejich nejvyššího soudu daní také převody kryptoměn na burzách.

Situace se v České republice změnila v roce 2017, a to s úpravou zákona o některých opatřeních proti legalizaci z výnosu z trestné činnosti a financování terorismu. Tento nový zákon definoval pojem „virtuální měna“ a z tohoto důvodu byla zavedena povinnost pro banky působící v České republice a kryptoměnové burzy nebo směnárny zaznamenávat totožnost klienta při směně kryptoměn nad částku 1000 €. Toto nařízení se ale netýká podniků nebo e-shopů, které poskytují za kryptoměny určitý druh služeb nebo zboží.

V případě, že osoba vlastní například 1 BTC jehož dnešní cena se pohybuje kolem 88 tisíc korun a prodá jej za tuto částku, tak se již jedná o příjem a daní se dle §10 Zákona o dani z příjmu. Co se týče těžby, jedná se o jednoznačně opakující se činnost, a tudíž je nutné si zřídit živnostenský list, jelikož těžba už se dá považovat za ekonomickou činnost. V případě, že tato vytěžená kryptoměna je následně směněna například za něco jiného, než je reálná měna (např. dům nebo auto), tak se jedná o zdanitelný příjem z těžby.

Na závěr se dá říci, že nákup nebo výměna kryptoměn není v České republice nijak zdaněna. Nicméně v případě, že je kryptoměna směněna za reálnou měnu, je osoba povinna tento zisk zdanit dle §10 Zákona o dani z příjmu. Podobná situace nastává u těžby. Díky malé regulaci kryptoměn se Česká republika stala domovem mnoha společností, které obchodují nebo těží kryptoměny. Vzhledem k tomu, že úřady nejsou kvůli složitému legislativními procesu schopny rychle reagovat na trendy, dá se předpokládat, že tento stav vydrží ještě nějakou dobu. Vzhledem

k tomu, že kryptoměny stále poskytují velkou možnost k daňovým únikům, dá se očekávat, že nás v nejbližších letech čeká stále větší regulace, jak ze strany legislativních norem EU, tak ze strany zákonů ČR. [24] [25]

7.2 V Evropské unii

Jak už bylo zmíněno v předchozí podkapitole 7.1, tak se všechny členské státy EU musí řídit závaznými legislativními normami. Evropská unie je stále v rané fázi regulace kryptoměn, což je vzhledem k rychlému nástupu kryptoměn a složitých legislativních procesech uvnitř EU očekávatelné. Z tohoto důvodu většina členů EU implementuje v rámci svých zákonů své vlastní řešení regulace kryptoměn.

Již v roce 2012 Evropská centrální banka vydala jako jedna z prvních takovýchto institucí zprávu pojmenovanou „Virtual Currency Schemes“, kde byl Bitcoin definován jako „typ neregulované digitální měny, která je vytvářena a povětšinou kontrolována jejími vývojáři, a je používána a přijímána členy v rámci specifické virtuální komunity“. V roce 2015 poté tuto zprávu aktualizovala a uvedla zde, že kryptoměny nejsou peníze, jelikož nesplňují tři pravidla, která jsou definována v ekonomických literaturách. Místo toho v této zprávě uvedla že virtuální měna (kryptoměna) je digitální reprezentací hodnoty, kterou nevydává žádná centrální banka nebo úvěrová instituce a může být v jistých případech využita jako alternativa peněz.

V roce 2016 Evropská komise navrhla a v roce 2017 přijala návrh, který definuje povinnost například kryptoměnovým burzám nebo směnárnám vyžadovat po uživatelích ověření své identity. Toto opatření je v drtivé většině případů dodržováno například tím, že uživatel musí nahrát oskenovaný doklad totožnosti, což je například občanský nebo řidičský průkaz.

Stejně jako v ČR jsou i v rámci EU kryptoměnové transakce osvobozeny od DPH. [26]

8 Implementace

V této kapitole bude popsána samotná implementace aplikace. Aplikace se skládá ze dvou části. První aplikace je takzvaný frontend, což je to, co uživatel vidí. V případě této aplikace se jedná o zjednodušenou podobu e-shopu, na kterém je možno nakoupit základní potraviny za pomoci kryptoměn. Druhou aplikací je logická část, a to backend, který své funkce zpřístupňuje na venek pomoci REST API.

Pro vytvoření frontend aplikace jsem si zvolil Node.js spolu s technologií React díky které jsem schopný vytvářet velice moderní single-page aplikace. V případě frontendu se každopádně jedna pouze o ukázkovou aplikaci a může být samozřejmě vzhledem k využití REST API vytvořena v jakémkoliv frameworku a jazyce.

Backend je vytvořen pomoci frameworku ASP.NET Core 2.1 a jazyka C#. Tento framework jsem si zvolil z důvodu mých pracovních zkušeností v této technologii. Zároveň je také C# velice moderním jazykem, který dovoluje psát výkonné aplikace v krátkém časovém horizontu. Výhodou nového ASP.NET Core je také to, že je možné spustit aplikaci také na Linux serveru nebo MacOS. Nejsme tedy jako tomu bylo v minulosti omezeni pouze na Windows. Díky REST API je aplikace velice univerzální, a v případě potřeby je možno aplikaci využít pro vlastní potřeby, například v rámci svého e-shopu, nebo vytvořit platební bránu jako službu pro veřejnost.

Vzhledem k tomu, že jsem si zvolil pracovat s ASP.NET Core byl jako databázový server zvolen Microsoft SQL server. Databáze je využívána pouze na straně backend aplikace, jelikož na straně frontendu to pro potřeby této diplomové práce potřeba není.

V rámci této kapitoly bude detailně popsáno, jak platební brána funguje, postup při implementaci, REST API burzy Binance, REST API směnárny Coinbase, kompletní implementaci kryptoměn, zvolené technologie a popis REST API funkcí a zabezpečení aplikace.

8.1 Popis platební brány

Platební brána, kterou jsem se rozhodl v rámci této diplomové práce vytvořit bude kromě klasických kryptoměn jako je Bitcoin, Ethereum nebo Litecoin podporovat také alternativní kryptoměny Ripple, Neo a Dash. Z tohoto důvodu je platební brána více použitelná pro větší počet potencionálních zákazníků. Zároveň se, ale také v rámci samotného procesu platby jedná o jeden krok navíc.

O kroku navíc se bavíme z toho důvodu, protože jsem si na směnu z kryptoměn na reálnou měnu vybral Coinbase, který ale nepodporuje v době psaní této diplomové práce tří kryptoměny Ripple, Neo a Dash. Z tohoto důvodu je potřeba udělat v rámci směny na reálnou měnu jeden krok navíc. V rámci tohoto mezikroku je potřeba při platbě jednou z těchto kryptoměn směnit tyto kryptoměny na Bitcoiny. Tyto Bitcoiny jsou následně odeslány do směnárny Coinbase a směněny za jednu z podporovaných světových měn což je v případě této aplikace euro. Pro směnu těchto tří kryptoměn na Bitcoin jsem si vybral burzu Binance, která zároveň podporuje

několik desítek různých kryptoměn, a z tohoto důvodu také nebude problém implementovat v budoucnu do platební brány více kryptoměn.

V několika bodech bude níže popsán obrázek č.21 tzn. jak celý proces platby funguje.

- Uživatel si zakoupí na e-shopu například ledničku. Tuto ledničku vloží do košíku a zvolí platbu kryptoměnami. Vzhledem k tomu, že zákazník těží kryptoměnu Dash, může si dovolit zakoupit ledničku právě za tuto kryptoměnu.

- Po zvolení kryptoměnu DASH je následně vyzván, aby zaslal částku 100 DASH na adresu XqHt831rFj5tr4PVjqEcJmh6VKvHP62QiM, a to do 20 min od vytvoření objednávky. Díky kurzovnímu lístku na stránce e-shopu zákazník dopředu věděl, že to bude přibližně tato částka.

- Nyní, když uživatel odeslal na adresu danou částku, čeká na potvrzení o platbě. Po přibližně dvou minutách je uživatel informován o tom, že platba proběhla v pořádku, a tímto platební proces pro zákazníka končí. V rámci algoritmu platební brány, ale proces zpracování teprve začíná.

- Jelikož uživatel zvolil kryptoměnu DASH, je potřeba co nejrychleji směnit DASH na Bitcoin. Algoritmus tedy odešle částku 100 DASH z peněženky, na kterou zákazník odeslal platbu na burzu Binance. Následně systém provede směnu dle aktuálního kurzu. Vzhledem k menším výkyvům kurzu je v celkové částce započítaná jistá rezerva, a to v hodnotě tří procent z celkové částky. Tato rezerva zajistí, že v rámci minut, kdy platba probíhá, nepřijde e-shop v případě kolísání kurzu o část svých peněz. Po úspešné směně jsou Bitcoiny odeslány do směnárny Coinbase. V případě, že by zákazník zvolil platbu Bitcoiny, Ethereem nebo Litecoiny, tak by se tento krok vynechal a kryptoměny by byly odeslány rovnou na Coinbase.

- V dalším kroku algoritmus provede směnu kryptoměny (v případě tohoto příkladu Bitcoinu) na reálnou měnu. Jelikož má Coinbase také poplatky, byly tyto poplatky zahrnuty do výsledné ceny. E-shop si každopádně může zvolit, zdali poplatky uhradí on nebo nakupující.

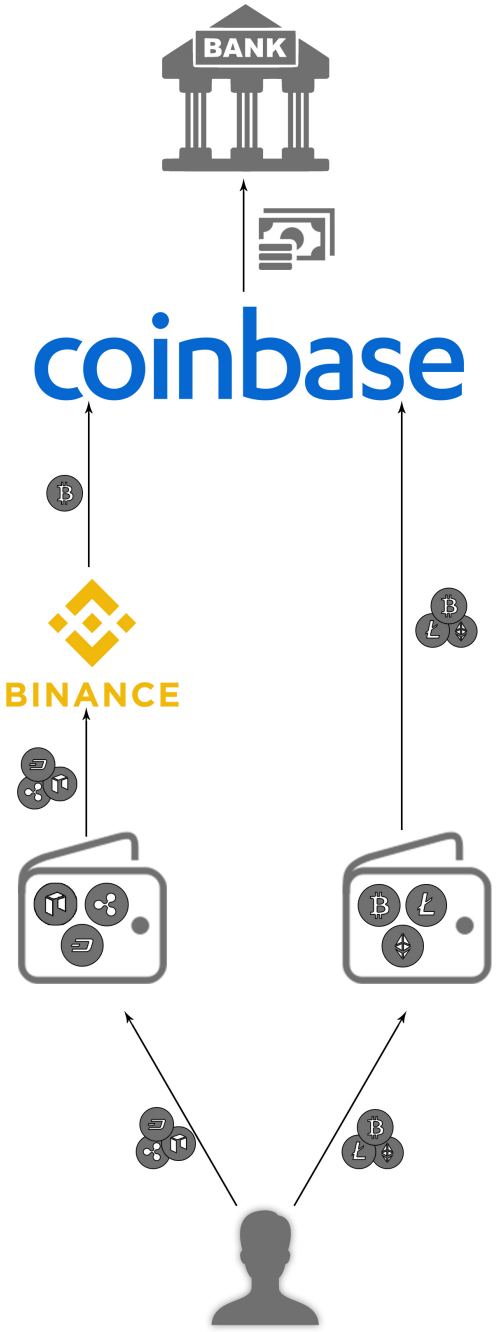
- Posledním krokem je poté v rámci výplat jednou měsíčně zaslat reálnou měnu, na účet e-shopu pomoci SEPA platby. Z celkové částky bude zároveň odečtena také provize pro poskytovatele platební brány v hodnotě 3% z celkové částky.

Tento popis byl tedy jakýmsi zjednodušeným popisem, jak platba v rámci této platební brány probíhá.

Jak už bylo zmíněno, e-shop (prodejce) si může v rámci platební brány zvolit, zdali chce poplatky za platbu hradit on nebo je má hradit kupující. Zároveň si také může e-shop zvolit, zdali chce kryptoměny směňovat na reálnou měnu. Je zde totiž možnost, že si chce směnu provést

sám, a proto je mu umožněno odeslat danou částku do své soukromé peněženky. V tomto případě by mu byly odpuštěny poplatky, které si účtuje Coinbase, respektive Binance. Jediný poplatek, který by mu byl odečten by byl poplatek ve výši 3% za využití naší platební brány a poplatek za převod kryptoměn mezi peněženkami.

Díky tomu, že byla logika platební brány naprogramována jako REST API, není žádný problém implementovat platební bránu v rámci jakéhokoliv webového frameworku. Informace o tomto REST API budou uvedeny v podkapitole 8.6.



Obrázek 21: Zjednodušený proces platby

8.2 Postup implementace

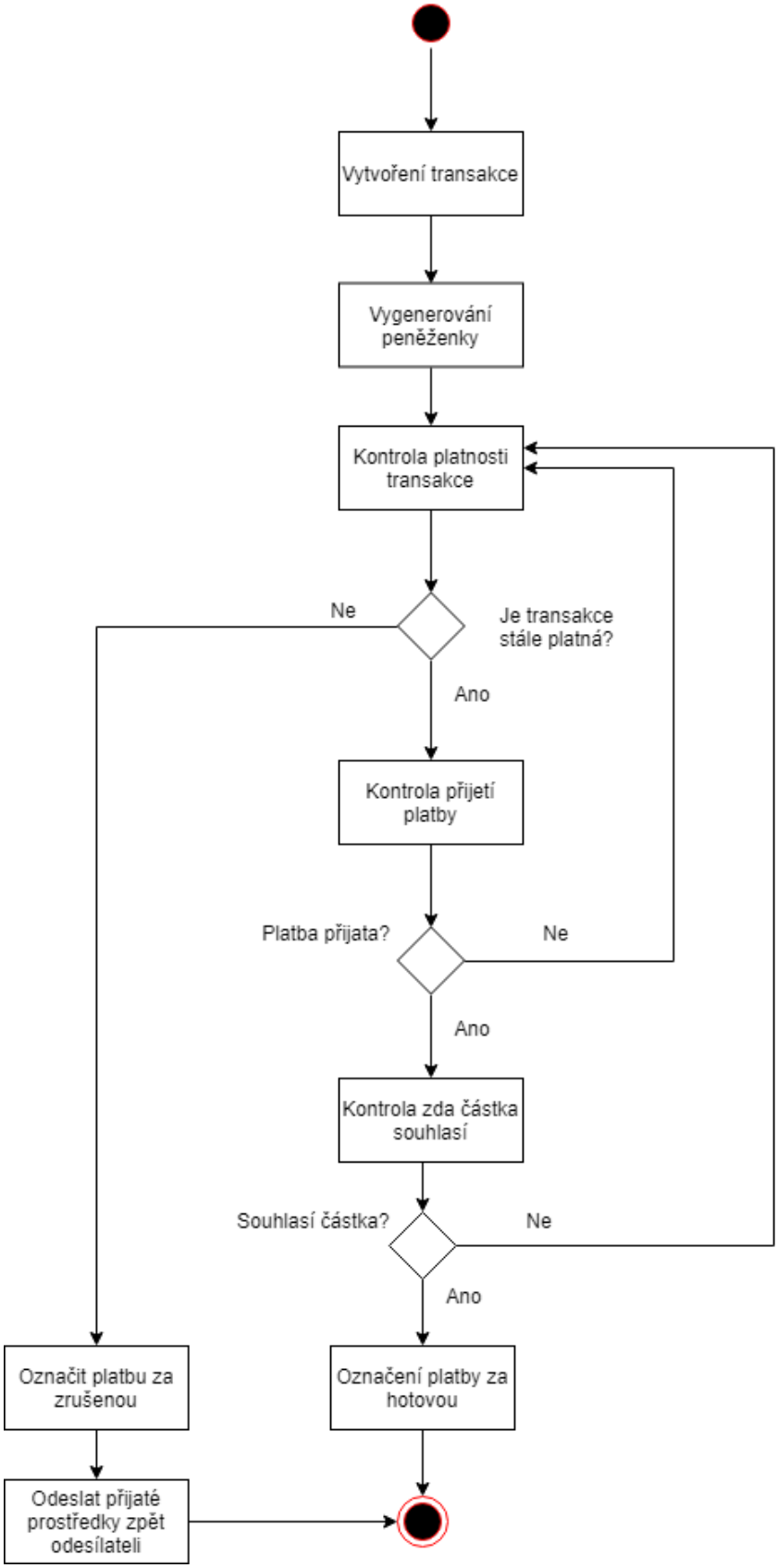
Vzhledem k tomu, že v dnešní době existuje již několik platebních bran čistě pro kryptoměny, předpokládálo se, že nebude nic jednoduššího než se inspirovat již hotovým řešením. Nicméně všechny platební brány vyžadují registraci společně s nutností mít minimálně IČO. Rozhodl jsem se tedy vymyslet si vlastní implementaci.

V první řadě jsem se rozhodl řešit způsob, jak vůbec kryptoměny přijímat. V prvotní fázi jsem narazil na problém, a to takový, že žádná z kryptoměn neumožňuje v rámci transakce zadat například variabilní symbol nebo poznámku, tak jako tomu je u obyčejných bankovních převodů. Nastal zde tedy zásadní problém, jak v rámci jednotlivých nákupů rozlišovat přijaté platby. Jako první mě napadlo rozlišovat platby pomocí částky. Jednoduše bych vždy vygeneroval náhodně několik desetinných míst a tím bych rozpoznal o kterou příchozí transakci se jedná. Pravděpodobně by se jednalo o řešení, které by fungovalo, ale stále by zde byl například problém, kdyby uživatel odeslal platbu například z dvou různých peněženek, a to by dle mého názoru mělo být umožněno. Dalším problémem by zde byla například i jistá estetičnost částky potřebná k zaplacení objednávky. Přece jen vypadá lépe částka 100 BTC než například 100,00026565. Z tohoto důvodu jsem se s touto variantou nespokojil a snažil jsem se přijít na lepší řešení.

Vzhledem k tomu, že pracuji s kryptoměnami, bylo potřebné si samozřejmě nastudovat, jak vůbec z technického hlediska kryptoměny fungují. Díky tomu jsem zjistil, že existuje možnost generovat nekonečné množství peněženek. Přišel jsem tedy na řešení, které nakonec bylo to správné. Při každé platbě generuji pro zvolenou kryptoměnu novou peněženku. Na základě adresy této peněženky je mimo jiné možno kontrolovat její zůstatek. To zákazníkovi zároveň umožňuje zaplatit objednávku z více peněženek, a to například proto, že většina majitelů kryptoměn má své kryptoměny umístěné ve více peněženkách z důvodu vyšší bezpečnosti a menšího rizika odcizení.

Nyní, když jsem věděl, jak rozlišit platby, bylo nutno také vyřešit, jakým způsobem zjistit, že převod kryptoměn úspěšně proběhl a já můžu objednávku označit jako zaplacenou.

Každá kryptoměna využívá tzv. blockchain [39]. Z tohoto důvodu existují webové služby, které umožňují tento blockchain procházet, a díky tomu vyhledávat peněženky včetně zůstatku nebo například informací o transakcích. Jedním z těchto block explorerů je https://chain.so, který byl využit pro ověření plateb v rámci kryptoměn Bitcoin, Litecoin a DASH. Toto ověření bylo provedeno pomocí volně dostupného REST API [33], které tato služba poskytuje. V první řadě je potřeba si dát pozor na takzvané konfirmace. V rámci kryptoměnových transakcí totiž probíhají konfirmace, které nám ověří platnost transakce. V případě, že proběhne alespoň 6 úspěšných konfirmací, tak je jisté, že je transakce pravá. V případě Chain.so nám každopádně jejich REST API vrací v parametru confirmed_balance pouze ověřený zůstatek peněženky. V případě, že se tedy hodnota tohoto paramteru rovná částce objednávky, tak je možno platbu označit jako přijatou.



Obrázek 22: Diagram aktivit - Postup ověření transakce

V případě kryptoměny NEO je využito oficiální RPC (vzdálené volání procedur), a to konkrétně v rámci main netu, což je hlavní kanál této kryptoměny (existuje také testovací síť tzv. test net).

Následně u kryptoměn Ethereum a Ripple byl opět využit podobný přístup jako je tomu u kryptoměn Bitcoin, Litecoin a DASH. To znamená, že je opět použit ke zjištění zůstatku v peněžence REST API, a to konkrétně v případě Etherea https://infura.io [34], a v případě kryptoměny Ripple je to oficiální REST API přímo od firmy Ripple [35].

V tento moment bylo možné potvrdit přijetí platby, a tím pádem se posunout k druhému kroku, což byl převod kryptoměny z peněženky, do které byla platba přijata. Samotná funkce odeslání kryptoměn do jiné peněženky je univerzální, a tudíž je možno odeslat libovolnou částku z dostupných prostředků do libovolné peněženky stejné kryptoměny. Odeslání kryptoměny bylo z programátorského hlediska o trochu složitější než předchozí krok, jelikož bylo potřeba provést více kroků. Stejně jako v předchozím kroku bylo v případě kryptoměn Bitcoin, Litecoin a DASH využito pro odeslání transakce do sítě REST API Chain.so a v případě Etherea, Ripple a NEO byly využity .NET knihovny.

Většina e-shopů, které chtějí přijímat kryptoměny, zároveň chce tyto kryptoměny okamžitě směnit, respektive nezajímají je samotné kryptoměny, ale pouze způsob, jak přijímat platby, které jim vygenerují zisk v reálné měně. Z tohoto důvodu bylo potřeba posunout se k dalšímu kroku, a to v rámci transakce směnit kryptoměnu v reálném čase za reálnou měnu. Po hlubší analýze všech směnáren byla využita ta nejznámější, a to Coinbase. Díky Coinbase bylo možné v rámci několika málo minut vyměnit kryptoměny za reálné peníze a následně je odeslat na bankovní účet. Coinbase zároveň poskytuje velmi propracované REST API, což bylo také jedním z důvodu volby teto směnárny. V případě plateb pomocí kryptoměn Bitcoin, Litecoin a Ethereum byl tedy postup jasný. Po přijetí do vygenerovaných peněženek okamžitě odeslat kryptoměny na Coinbase, kde budou následně směněny na reálnou měnu. Tento postup ale nebyl možný u kryptoměn NEO, Ripple a DASH, jelikož je Coinbase nepřijmá.

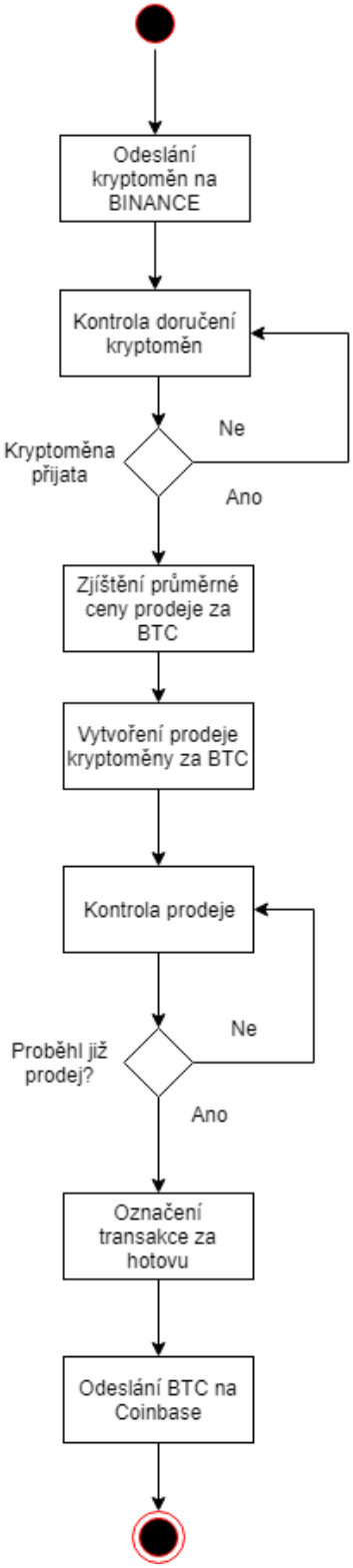
Tabulka 1: Poplatky směnárny Coinbase

	<= 10€	<= 25€	<= 50€	<= 20€	>200€
Poplatek za výměnu BTC	0.99€	1.49€	1.99€	2.99€	1.49% z celkové částky
Poplatek za odeslání financí na účet - 0.15€					

Rozhodl jsem se tedy pro tyto tři kryptoměny provést mezikrok v rámci zpracování celé platby. Po přijetí těchto kryptoměn jsou kryptoměny odeslány na burzu Binance, kde jsou následně směněny za kryptoměnu Bitcoin. Tyto Bitcoiny jsou následně odeslány do směnárny Coinbase a směněny na reálnou měnu. V rámci této varianty každopádně nastává jistý problém. Tím problémem je že je zde další služba, která si naúčtuje jakési poplatky. V tomto případě jsou to poplatky burzy Binance. Bylo tedy nutné započítat tyto poplatky do celkové částky a tím pádem by se dalo říci, že je kupující (nebo prodávající) trochu znevýhodněn oproti tomu, kdyby platil pomocí Bitcoinu, Litecoinu nebo Etherea. Je to každopádně na zákazníkovi, jestli si zvolí platit pomocí jedné z těchto tří kryptoměn.

Tabulka 2: Poplatky burzy Binance

Poplatek za výměnu všech kryptoměn	0,1 %
Deposit (příjem kryptoměn)	zdarma
Poplatek za výběr (odeslání) BTC	0.0005 BTC (min. výběr 0.002 BTC)

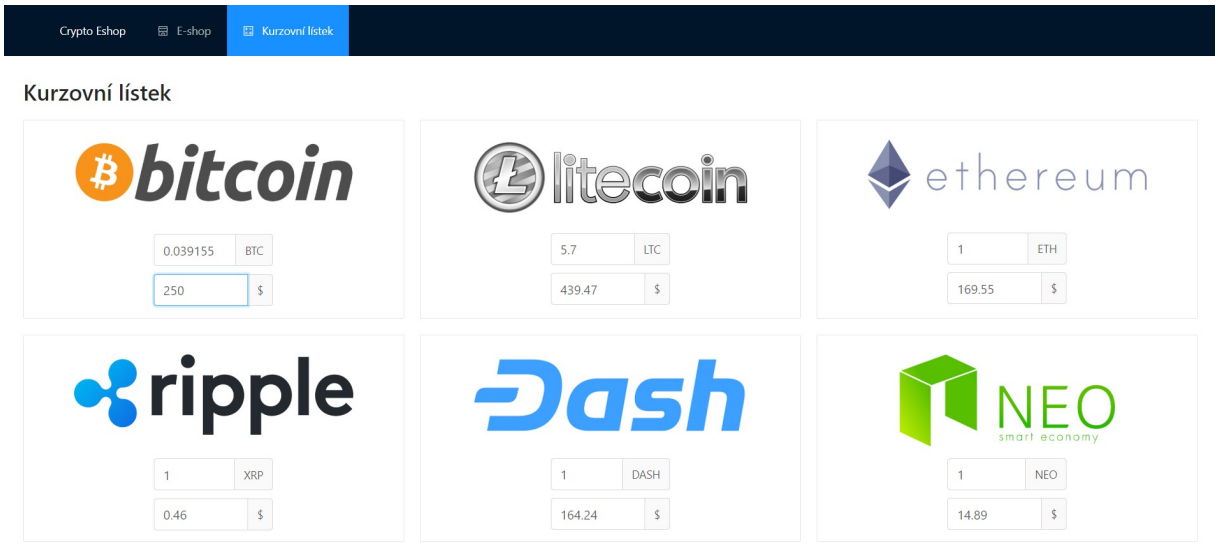


Obrázek 23: Diagram aktivit - Postup směny v rámci burzy Binance

Posledním zásadním krokem ve zpracování platby je odeslání reálné měny na bankovní účet daného e-shopu. Tyto převody jsou ze strategických důvodů odesílány jednou týdně. Jedná se o logický krok, jak už z pohledu fakturace, tak přehlednosti. Přece jen je lepší odesílat výdělek e-shopu v určitém intervalu. Ostatně, není to nic nového, jelikož tento způsob výplat využívají i klasické platební brány, jako je například GoPay.

V tuto chvíli byl tedy celý proces platby hotový. Nicméně se jednalo pouze o první část implementace platební brány. Druhou části bylo samotné zabezpečení platební brány. Je tedy třeba v rámci REST API nějakým způsobem rozeznat, o jaký e-shop v rámci platby se vůbec jedná. V případě, kdybych nějakým způsobem neautentizoval uživatele v rámci REST API, nevěděl bych pro jaký e-shop je daná platba určena. Díky mým pracovním zkušenostem jsem se v rámci REST API již setkal s autentizací pomocí JWT tokenu a rozhodl jsem se tento způsob autentizace využít také v rámci této aplikace.

V první řadě, aby e-shop mohl vůbec využívat platební bránu musí se zaregistrovat a poskytnout mi údaje jako je název firmy, IČO, adresu, číslo bankovního účtu a podobně. Po úspěšné registraci se uživateli, což je v tomto případě e-shop, vygeneruje JWT token. Tento JWT token je poté potřeba zahrnout do HTTP hlavičky každého dotazu na REST API platební brány, a to konkrétně jako hlavičku Authorization s hodnotou „Bearer [JWT TOKEN]“. Tímto si zajistím, že do backend aplikace nebude mít přístup nikdo, kdo nemá oprávnění, respektive není zaregistrován. Uživateli se také vygenerují peněženky pro každou kryptoměnu. Tyto peněženky budou na stálo svázaný s uživatelem a bude si do nich moci nechat posílat kryptoměny v případě, že si nebude přát provádět směnu. K těmto peněženkám bude mít zároveň přístup a bude moci provádět výběry. Zároveň si uživatel bude moci nastavit, zdali chce kryptoměny směňovat anebo si je nechávat. Dalším volitelným nastavením je také možnost zvolit si, zdali poplatky za platbu zaplatí sám e-shop nebo nakupující.



Obrázek 24: Aplikace - ukázka kurzovního lístku

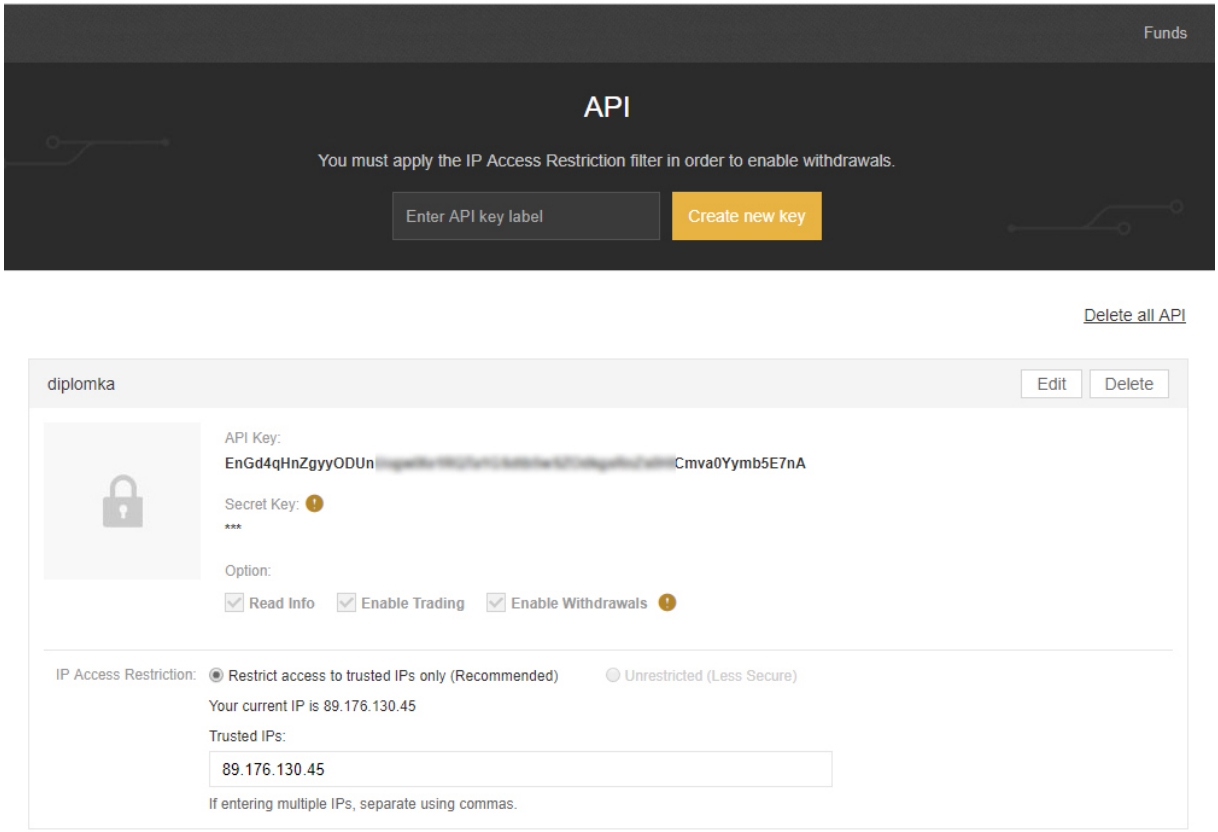
Poslední věci, kterou bylo potřeba naimplementovat je živý kurzovní lístek. Tento kurzovní lístek může e-shop využít pro zobrazení aktuální ceny včetně poplatků v rámci libovolné kryptoměny. Zároveň může také uživatelům poskytnout kalkulačku díky které si můžou zjistit uživatelé v rámci jaké kryptoměny je platba vyjde z finančního hlediska nejlépe.

8.3 Burza Binance a její API

Burzu Binance jsem si zvolil pro směnu kryptoměn NEO, Ripple a DASH na kryptoměnu Bitcoin. Z tohoto důvodu bylo potřeba implementovat tuto burzu do automatického procesu zpracování transakce. Tuto implementaci jsem zrealizoval pomoci REST API, které Binance poskytuje.

Binance stejně jako většina poskytuje dokumentaci ke svému REST API, a to na webové stránce [37]. Dokumentace je zpracována v celku dobře, ale není zde vždy úplně vše vysvětleno. Je tedy potřeba mít nějaké znalosti a zkušenosti s REST API, aby člověk mohl toto REST API bez problému implementovat.

Pro potřeby platební brány byly využity celkem čtyři funkce, které Binance REST API poskytuje. Před tím, než samotné REST API začneme využívat je potřeba se samozřejmě zaregistrovat. Registrace na burze je oproti jiným webům trochu zdlouhavější. Jak už bylo zmíněno v předešlých kapitolách, je potřeba nahrát dva dokumenty totožnosti, a to z důvodu opatření proti praní špinavých peněz.



Obrázek 25: Vytvoření API přístupu na burze Binance

Po úspěšné registraci a přihlášeni je potřeba vygenerovat REST API klič. Tento klíč slouží při voláni REST API k ověření naší totožnosti, a tím pádem získání dat vázaných k našemu účtu. Společně s tímto API klíčem obdržíme také tak zvaný secret key. Tento secret key uvidíme pouze jednou a je potřeba si ho uložit na velice bezpečné místo. Klíč jsem se rozhodl v rámci aplikace uložit pomoci secret manager toolu [40], který je součástí visual studia potažmo ASP.NET Core. V případě, že by útočník zjístí tento secret key, tak je to první krok k odcizeni kryptoměn. Druhým zabezpečením, které Binance poskytuje je omezení přístupu na API pomoci IP adresy, které jsem také využil.

Zároveň na obrázku č.24 můžeme vidět možnost nastavit si omezení API na jednotlivé akce (obchodování, výběr, čtení). Pro potřeby naší aplikace byly využity všechny tři možnosti.

Z důvodu jednoduššího využití REST API jsem se rozhodl použít .NET knihovnu Binance.Net
(https://github.com/JKorf/Binance.Net). Díky této knihovně je volání REST API funkcí přehlednější. Zároveň v rámci autentizace stačí pouze jako parametr funkce předat API klíče.

První REST API funkci, která byla využita, je funkce na zjištění aktuální ceny kryptoměny na burze. Tato funkce je interně využívána ke zjištění aktuální ceny směny, a díky tomu je možné vypočítat cenu nákupu. Funkci jsem se rozhodl implementovat velmi univerzálně, a proto je možné díky ní zjistit cenu jakékoliv podporované kryptoměny vůči jiné kryptoměně. Nás primárně ale zajímá DASH->BTC, XRP->BTC a NEO->BTC.

Binance REST API

HTTP adresa: GET https://api.binance.com/api/v3/ticker/price
Parametry:

Tabulka 3: Použité parametry Binance API - price

Název	Datový typ	Povinný	Poznámka
symbol	String	Ano	např. DASHBTC, XRPBTC...

Odpověď:

```
{
  "symbol": "DASHBTC",
  "price": "4.00000200"
}
```

Výpis 1: Odpověď Binance API - price

Další REST API funkce, kterou bylo potřeba využit, je funkce na zjištění příchozích plateb v rámci Binance peněženky dané kryptoměny. Tato funkce slouží ke zjištění, zda byla transakce uskutečněna. V našem případě se jedná o transakci z vygenerované peněženky dané kryptoměny, v rámci které byly převedeny prostředky do naší peněženky na burze Binance. Tato funkce je volána opakovaně, jelikož u každé kryptoměny trvá potvrzení platby různě dlouho. Tato funkce je opět využita pouze interně, a to při procesování transakce. To znamená, že e-shop, který implementuje naši platební bránu na tuto funkci tak zvaně "nevidí". Oproti předchozí funkce, kterou bylo možno volat bez autentizace je v tomto případě potřeba již poskytnout v hlavičce dotazu autentizační "API key"a "secret KEY". V předchozím volání API funkce jsem se rozhodl v rámci kódu volat tuto funkci jako obyčejný HTTP požadavek. V případě této funkce již byla z důvodu potřeby autentizace využita dříve zmiňovaná .NET knihovna Binance.NET.

Binance REST API

Název funkce GetDepositHistoryAsync (GET /wapi/v3/depositHistory.html)
Parametry:

Tabulka 4: Použité parametry Binance API - GetDepositHistoryAsync

Název	Datový typ	Povinný	Poznámka
asset	String	Ne	např. DASH, XRP, NEO...

Ukázka kódu:

```
using (var client = new BinanceClient())
{
   client.SetApiCredentials(API_KEY, SECRET_KEY);
   string asset = "ETH";
   CallResult<BinanceDepositList> history = await client.
      GetDepositHistoryAsync(asset);
}
```

Výpis 2: Binance.NET - GetDepositHistoryAsync

Odpověď:


```
{
    "depositList": [
        {
            "insertTime": 1508198532000,
            "amount": 0.04670582,
            "asset": "ETH",
            "address": "0x6915f16f8791d0a1cc2bf47c13a6b2a92000504b",
            "txId": "0xdf33b22bdb2b28b1f7jy5fc5d5a9d1340961598cfcb0a1",
            "status": 1
        }
    ],
    "success": true
}
```


Výpis 3: Odpověď Binance API - GetDepositHistoryAsync

Následuje jedna z nejdůležitějších funkcí, a to funkce na zahájení, respektive odeslání nabídky výměny dané kryptoměny za Bitcoin. Tato funkce vytvoří nabídku výměny, respektive prodeje v reálném čase. Nabídka bude platná do doby, než bude provedena nebo zrušena. V případě této diplomové práce je cena prodeje vždy nižší než aktuální cena. To zaručuje rychlý a bezproblémový prodej na úkor několika málo centů. Zároveň může tato funkce sloužit k vytvoření příkazu k nákupu, ale tato možnost v rámci této diplomové práce nebude využita.

Binance REST API

Název funkce PlaceOrderAsync (POST /api/v3/order)
Parametry:

Tabulka 5: Použité parametry Binance API - PlaceOrderAsync

Název	Datový typ	Povinný	Poznámka
symbol	String	Ano	DASHBTC, XRPBTC, NEOBTC
side	Enum	Ano	Sell, Buy
type	Enum	Ano	limit (typ prodeje)
quantity	Decimal	Ano	Množství k prodeji
timeInForce	Decimal	Ne	Good till cancel (aktivní dokud neproběhne nebo se nezruší)
price	Decimal	Ne	Prodejní cena (snížena o 0.05%)

Ukázka kódu:

```
using (var client = new BinanceClient())
{
   client.SetApiCredentials(API_KEY, SECRET_KEY);
   CallResult<BinancePrice> DashBtcPrice = await client.
       GetPriceAsync("DASHBTC");
      CallResult<BinancePlacedOrder> order = await client.
         PlaceOrderAsync("DASHBTC", OrderSide.Sell,
       type: OrderType.Limit,
       quantity: 0.12m,
       timeInForce: TimeInForce.GoodTillCancel,
       price: DashBtcPrice.Data.Price - (DashBtcPrice.Data.Price *
           0.05)
       );
}
```

Výpis 4: Binance.NET - PlaceOrderAsync

Odpověď:


```
{
  "symbol": "DASHBTC",
  "orderId": 28,
  "clientOrderId": "6gCrw2kRUAF9CvJDGP16IP",
  "transactTime": 1507725176595,
  "price": "1.00000000",
  "origQty": "10.00000000",
  "executedQty": "10.00000000",
  "cummulativeQuoteQty": "10.00000000",
  "status": "FILLED",
  "timeInForce": "GTC",
  "type": "MARKET",
  "side": "SELL"
}
```


Výpis 5: Odpověď Binance API - PlaceOrderAsync

V návaznosti na předchozí funkci je zároveň nutno zjistit, zda prodej proběhl úspěšně, nebo je stále neproveden. Tato funkce tedy umožní zjistit, zda algoritmus může pokračovat k dalšímu kroku, což je převod získaných Bitcoinu do směnárny Coinbase. Funkce by měla být volána v určitém časovém intervalu, a to z toho důvodu, že prodej většinou trvá několik minut. Tento čas velice závisí na stanovené prodejní ceně. V případě této diplomové práce je aktuální prodejní cena snížena o 0.05%. To znamená, že pravděpodobnost rychlého prodeje je vyšší.

Binance REST API

Název funkce QueryOrderAsync (GET /api/v3/order)
Parametry:

Tabulka 6: Použité parametry Binance API - QueryOrderAsync

Název	Datový typ	Povinný	Poznámka
symbol	String	Ano	DASHBTC, XRPBTC, NEOBTC
orderId	Long	Ano	Id prodeje získáno při vytvoření prodeje

Ukázka kódu:

```
using (var client = new BinanceClient())
{
   client.SetApiCredentials(API_KEY, SECRET_KEY);
   CallResult<BinanceOrder> orderInfo = await client.QueryOrderAsync
       ("DASHBTC", 28);
}
```

Výpis 6: Binance.NET - QueryOrderAsync

Odpověď:


```
{
  "symbol": "DASHBTC",
  "orderId": 28,
  "clientOrderId": "myOrder1",
  "price": "0.1",
  "origQty": "1.0",
  "executedQty": "0.0",
  "cummulativeQuoteQty": "0.0",
  "status": "NEW",
  "timeInForce": "GTC",
  "type": "LIMIT",
  "side": "BUY",
  "stopPrice": "0.0",
  "icebergQty": "0.0",
  "time": 1499827319559,
  "updateTime": 1499827319559,
  "isWorking": true
}
```


Výpis 7: Odpověď Binance API - QueryOrderAsync

Poslední Binance REST API funkce, která byla v rámci diplomové práce využita, je funkce na výběr, respektive převod směněných Bitcoinů. V případě této varianty nákupu se jedná o převod Bitcoinů do směnárny Coinbase, a to k výměně (prodeje) za reálnou měnu. Po vytvoření požadavku na odeslání a následnému vrácení odpovědi success není již potřeba kontrolovat, zda transakce proběhla. Tato kontrola následně proběhne až na straně Coinbase.

Binance REST API

Název funkce WithdrawAsync (POST /wapi/v3/withdraw.html)
Parametry:

Tabulka 7: Použité parametry Binance API - WithdrawAsync

Název	Datový typ	Povinný	Poznámka
asset	String	Ano	BTC
address	String	Ano	Adresa příjemce
amount	Decimal	Ano	Množství BTC

Ukázka kódu:

```
using (var client = new BinanceClient())
{
   client.SetApiCredentials(API_KEY, SECRET_KEY);
   CallResult<BinanceWithdrawalPlaced> withdraw = await client.
      WithdrawAsync("BTC", "LiHfZuoZeg95CzJ5dtXV1D89pm5fsX42tt",
      0.15m);
}
```

Výpis 8: Binance.NET - WithdrawAsync

Odpověď:

```
{
    "msg": "success",
    "success": true,
    "id":"7213fea8e94b4a5593d507237e5a555b"
}
```

Výpis 9: Odpověď Binance API - WithdrawAsync

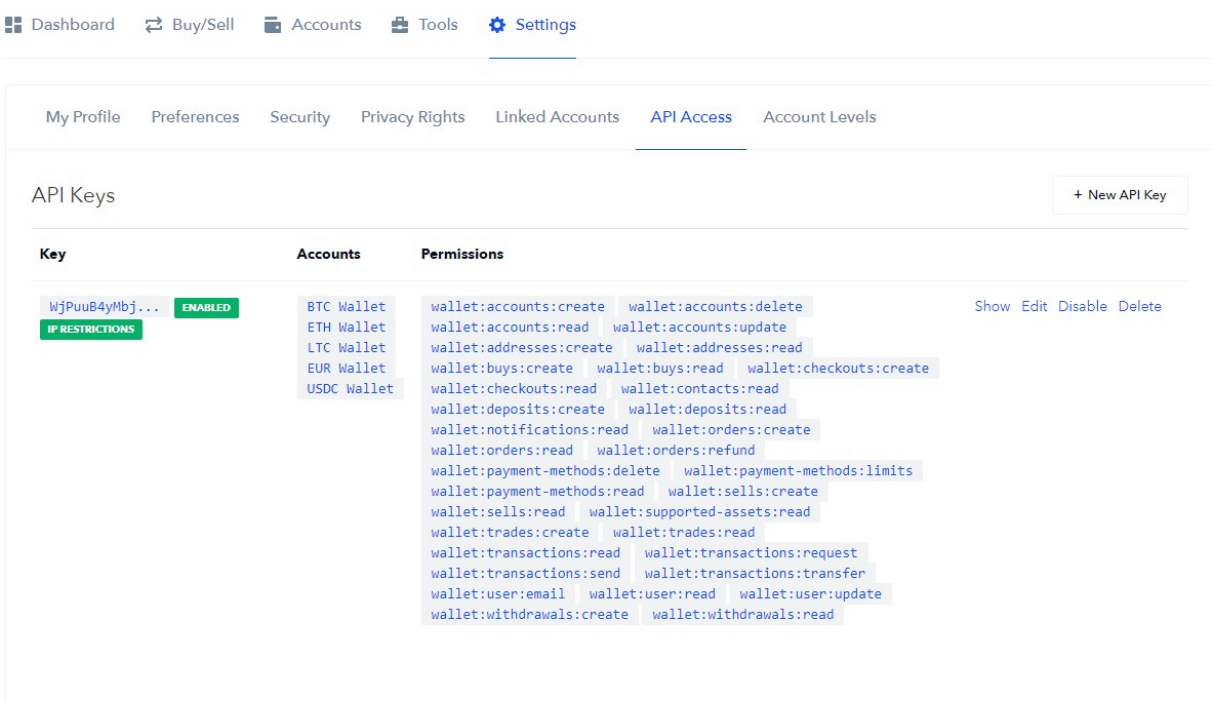
S výjimkou první funkce na zjištění ceny není ani jedna z těchto funkcí veřejná. To znamená, že e-shop, který bude implementovat tuto platební bránu, nemá přístup k využití těchto funkcí. Jedná se pouze o interní volání v rámci algoritmu aplikace.

V rámci diplomové práce nebylo potřeba využívat jiných API funkcí burzy Binance, ačkoliv jich poskytuje mnohem více.

8.4 Směnárna Coinbase a její API

Směnárna Coinbase je posledním krokem v procesu platby pomoci platební brány, která byla naprogramována v rámci této diplomové práce. Stejně jako tomu je u burzy Binance bylo u směnárny Coinbase využita REST API, které Coinbase poskytuje.

Prvním krokem potřebným pro využití služeb Coinbase směnárny je registrace. Registrace probíhá opět s nutností dodání fotografií dvou dokumentů totožnosti (například občanský a řidičský průkaz). Po úspěšné registraci a přihlášení je potřeba navštívit sekci nastavení a v ní sekci „API Access“. Následně je potřeba vygenerovat API a secret key. Díky těmto dvou klíčům jsme schopni autentizace našeho účtu v rámci Coinbase REST API. Důležité je také zvolit přístupová práva. Tyto práva nám určí, co všechno za pomocí tohoto API klíče budeme schopni dělat. V případě této diplomové práce byla zvolena plná práva bez omezení. Zároveň také byla využita tak zvaná IP restrikce což znamená, že na API s daným API klíčem bude možno přistupovat pouze z konkrétních IP adres. Současně je také potřeba vybrat které kryptoměny a měny v rámci API klíče budeme moci obsluhovat. V tomto případě byly z kryptoměn zvoleny Bitcoin, Litecoin a Ethereum. V rámci měn bylo poté zvoleno Euro.



Obrázek 26: Coinbase - založení API přístupu

Samotné API jsem se rozhodl stejné jako tomu bylo u Binance implementovat pomocí .NET knihovny Coinbase.NET (https://github.com/bchavez/Coinbase). Tento způsob jsem využil díky jednoduššímu volání API funkcí bez nutnosti vytvářet nové modely v rámci kódu. Dalším důvodem bylo také to že Coinbase v hlavičce každého dotazu vyžaduje tzv. podpis. Tento podpis je sha256 hash který je tvořen spojením údajů timestamp + method + requestPath + body. V případě knihovny je tento algoritmus vyřešen a plně automatizován, a díky tomu stačí pouze poskytnout API a secret key.

```
CoinbaseClient api = new CoinbaseClient(new ApiKeyConfig()
      {
          ApiKey = "WjfdsjDk9C3S6ddsC6dgLHpz"
          ApiSecret = "p4gcDtesNTINDc69eApC3s6c9tgyS"
       });
```

Výpis 10: Coinbase.NET - Inicializace API klienta

Jednou z prvních funkcí, kterou bylo potřeba implementovat je funkce na zjištění aktuálních cen ve směnárně Coinbase. Tato funkce je především využívána při výpočtu ceny transakce. Díky teto funkci můžeme vypočítat přibližnou cenu výměny kryptoměn za reálnou měnu. Zároveň je tuto funkci možno volat v rámci kurzovního lístku. Funkce není veřejně přístupná klientům, ale využívá se pouze interně.

Coinbase REST API

Název funkce GetSellPriceAsync (GET v2/prices/:currency_pair/sell)
Parametry:

Tabulka 8: Použité parametry Coinbase API - GetSellPriceAsync

Název	Datový typ	Povinný	Poznámka
:currency_pair	String	Ano	BTC-USD, ETH-EUR...

Ukázka kódu:

```
CoinbaseClient api = new CoinbaseClient(new ApiKeyConfig()
      {
          ApiKey = "WjfdsjDk9C3S6ddsC6dgLHpz"
          ApiSecret = "p4gcDtesNTINDc69eApC3s6c9tgyS"
       });

Response<Money> btcUsd = await api.Data.GetSellPriceAsync("BTC-USD");
```

Výpis 11: Coinbase.NET - GetSellPriceAsync

Odpověď:

```
{
  "data": {
    "amount": "1010.25",
    "currency": "USD"
  }
}
```

Výpis 12: Odpověď Coinbase API - GetSellPriceAsync

Po odeslání prostředků na Coinbase je potřeba zjistit, zda prostředky dorazily v pořádku a jsou k dispozici. K tomu slouží funkce, která vypíše přijaté transakce. Na základě tohoto seznamu je možno zjistit, zda prostředky dorazily a je možno provést výměnu na reálnou měnu. Každá kryptoměna má v rámci Coinbase svojí vlastní peněženku. Z tohoto důvodu je potřeba kontrolovat všechny kryptoměny, které jsou v rámci Coinbase využívány, a to je Bitcoin, Litecoin a Ethereum. Funkce bude tedy volána v rámci algoritmu celkem třikrát. Funkce je využívána pouze v rámci algoritmu a není tudíž veřejně přístupná pomocí REST API.

Coinbase REST API

Název funkce ListDepositsAsync (GET v2/accounts/:account_id/deposits)
Parametry:

Tabulka 9: Použité parametry Coinbase API - ListDepositsAsync

Název	Datový typ	Povinný	Poznámka
:account_id	String	Ano	Id účtu dané kryptoměny v rámci účtu Coinbase

Ukázka kódu:

```
PagedResponse<Account> accounts = await api.Accounts.ListAccountsAsync();
Account ltcWallet = accounts.Data.FirstOrDefault(x => x.Name == "LTC Wallet");
if (ltcWallet != null)
{
PagedResponse<Deposit> deposits = await api.Deposits.ListDepositsAsync(
    ltcWallet.Id);
}
```

Výpis 13: Coinbase.NET - ListDepositsAsync (Litecoin)

Odpověď:


```
{
  "pagination": {...}
  "data": [
    {
      "id": "67e0eaec-07d7-54c4-a72c-2e92826897df",
      "status": "completed",
      "payment_method": {...},
      "transaction": {
        "id": "441b9494-b3f0-5b98-b9b0-4d82c21c252a",
        "resource": "transaction",
        "resource_path": "..."
      },
      "amount": {
        "amount": "10.00",
        "currency": "LTC"
      },
      "subtotal": {
        "amount": "10.00",
        "currency": "LTC"
      },
      .
      .
      .
      "fee": {
        "amount": "0.00",
        "currency": "USD"
      },
      "payout_at": "2019-02-18T16:54:00-08:00"
    }
  ]
}
```


Výpis 14: Odpověď Coinbase API - ListDepositsAsync (Litecoin)

Předposlední funkcí, která bude v rámci Coinbase v této diplomové práci využita, je funkce na zadání prodeje kryptoměny. Tato funkce umožňuje prodat kryptoměny, což je v našem případě Bitcoin, Litecoin a Ethereum za reálnou měnu (EUR). Výhodou tohoto prodeje je rychlost, jelikož každý prodej na Coinbase je okamžitý. Nevýhodou jsou poplatky, které nicméně byly

započítaný do celkové ceny transakce. Jedním z důležitých parametrů je payment_method, což je unikátní id EUR peněženky v rámci Coinbase. Tento parametr určí to, že za prodanou kryptoměnu budou získány eura.

Coinbase REST API

Název funkce PlaceSellOrderAsync (POST v2/accounts/:account_id/sells)
Parametry:

Tabulka 10: Použité parametry Coinbase API - PlaceSellOrderAsync

Název	Datový typ	Povinný	Poznámka
:account_id	String	Ano	Id účtu dané kryptoměny v rámci účtu Coinbase
amount	String	Ano	Množství kryptoměny
currency	String	Ano	BTC, ETH, LTC...
payment_method	String	Ano	Id EUR účtu v rámci Coinbase
commit	Boolean	Ano	True = prodej okamžitý, False = prodej odložený

Ukázka kódu:

```
PagedResponse<Account> accounts = await api.Accounts.ListAccountsAsync();
Account ltcWallet = accounts.Data.FirstOrDefault(x => x.Name == "LTC Wallet");
if (ltcWallet != null)
{

var placeOrder = new PlaceSell()
  {
     Amount = "10",
     Currency = "LTC",
     PaymentMethod = "c3e2b740-ee4b-54f6-acf4-87b20081ad92", // EUR učet
     Commit = true
  };

Response<Sell> sell = await api.Sells.PlaceSellOrderAsync(ltcWallet.Id,
    placeOrder);

}
```

Výpis 15: Coinbase.NET - PlaceSellOrderAsync (Litecoin -> EUR)

Odpověď:


```
{
  "data": {
    "id": "a333743d-184a-5b5b-abe8-11612fc44ab5",
    "status": "completed",
    "payment_method": {
      "id": "c3e2b740-ee4b-54f6-acf4-87b20081ad92",
      "resource": "payment_method",
      "resource_path": "..."
    },
    "transaction": {
      "id": "763d1401-fd17-5a18-852a-9cca5ac2f9c0",
      "resource": "transaction",
      "resource_path": "..."
    },
    "amount": {
      "amount": "10.00000000",
      "currency": "LTC"
    },
    "total": {
      "amount": "490.00",
      "currency": "EUR"
    },
    "created_at": "2019-04-01T18:43:37-07:00",
    "updated_at": "2019-04-01T18:43:37-07:00",
    "resource": "sell",
    "resource_path": "...",
    "committed": true,
    "instant": true,
    "fee": {
      "amount": "10.1",
      "currency": "EUR"
    },
    "payout_at": "2019-04-07T18:43:37-07:00"
  }
}
```


Výpis 16: Odpověď Coinbase API - PlaceSellOrderAsync (Litecoin -> EUR)

Poslední využitou funkcí v rámci Coinbase je funkce na výběr (převod) směněných finančních prostředků na reálný bankovní účet. Vzhledem k tomu, že Coinbase nepodporuje vytváření účtů v rámci svého API, je nutno všechny prostředky zasílat na jeden bankovní účet, ze kterého budou následně v již zmíněných časových intervalech odesílány dále klientům platební brány (e-shopům). Při tomto odeslání může také dojít ke směně na jinou světovou měnu. Tento krok každopádně neprovádí již samotná platební brána, ale jiný systém (např. účetní).

Coinbase REST API

Název funkce WithdrawalFundsAsync (POST v2/accounts/:account_id/withdrawals)
Parametry:

Tabulka 11: Použité parametry Coinbase API - WithdrawalFundsAsync

Název	Datový typ	Povinný	Poznámka
:account_id	String	Ano	Id účtu dané měny v rámci účtu Coinbase
amount	String	Ano	Množství
currency	String	Ano	EUR
payment_method	String	Ano	Id BANK účtu v rámci Coinbase
commit	Boolean	Ano	True = výběr okamžitý, False = výběr odložený

Ukázka kódu:

```
PagedResponse<Account> accounts = await api.Accounts.ListAccountsAsync();
Account eurWallet = accounts.Data.FirstOrDefault(x => x.Name == "EUR Wallet");
if (eurWallet != null)
{

var withdrawalFunds = new WithdrawalFunds()
{
   Amount = 100,
   Currency = "EUR",
   PaymentMethod = "83562370-3e5c-51db-87da-752af5ab9559", // BANK (FIAT) učet
   Commit = true
};
var withdraw = await api.Withdrawals.WithdrawalFundsAsync(eurWallet.Id,
    withdrawalFunds);
}
```

Výpis 17: Coinbase.NET - WithdrawalFundsAsync (EUR)

Odpověď:


```
{
  "data": {
    "id": "67e0eaec-07d7-54c4-a72c-2e92826897df",
    "status": "completed",
    "payment_method": {
      "id": "83562370-3e5c-51db-87da-752af5ab9559",
      "resource": "payment_method",
      "resource_path": "..."
    },
    "transaction": {
      "id": "441b9494-b3f0-5b98-b9b0-4d82c21c252a",
      "resource": "transaction",
      "resource_path": "..."
    },
    "amount": {
      "amount": "100.00",
      "currency": "EUR"
    },
    "created_at": "2019-01-31T20:49:02Z",
    "updated_at": "2019-02-11T16:54:02-08:00",
    "resource": "withdrawal",
    "resource_path": "...",
    "committed": true,
    "fee": {
      "amount": "0.00",
      "currency": "EUR"
    },
    "payout_at": "2019-02-18T16:54:00-08:00"
  }
}
```


Výpis 18: Odpověď Coinbase API - WithdrawalFundsAsync (EUR)

8.5 Implementace kryptoměn

Samotná implementace kryptoměn byla v rámci této diplomové práce nejsložitější částí. Každá z vybraných kryptoměn (kromě Bitcoinu a Litecoinu) pracuje na trochu jiném principu. Bylo potřeba tudíž nastudovat a naimplementovat každou z kryptoměn zvlášť. U každé kryptoměny bylo potřeba implementovat tři samostatné funkce, a to založení peněženky, zjištění stavu peněženky (zůstatek) a převod z prostředků z peněženky do peněženky (Coinbase, Binance). Všechny tyto funkce byly implementovány v rámci REST API kromě jedné, a to vygenerování Ripple peněženky. Tato funkce byla implementována v rámci node.js aplikace, která slouží jako ukázkový e-shop, jelikož se mi implementace této funkce v rámci backend aplikace nepodařila.

Bitcoin:
Pro implementaci Bitcoin funkcí byla využita knihovna NBitcoin [38], díky které bylo možné vygenerovat novou peněženku a vytvořit transakci mezi peněženkami. Pro odeslání určité částky do jiné peněženky je v případě Bitcoinu potřeba nejdříve zjistit všechny předchozí pohyby v rámci peněženky tzv. UTXO (Unspent Transaction Output). Tyto pohyby jsou následně v samotné transakci obsaženy. To ve výsledku znamená, že každá transakce obsahuje kompletní přehled pohybu dané peněženky.

```
Key privateKey = new Key(); //Vytvoření private key
BitcoinAddress address = privateKey.PubKey.GetAddress(Network.Main); //Adresa
BitcoinSecret secret = privateKey.GetBitcoinSecret(Network.Main); // Secret key
```

Výpis 19: Bitcoin vygenerování nové peněženky

Zůstatek peněženky následně pomocí REST API zjistíme díky službě Chain.so. Díky tomuto exploreru je možno zjistit zůstatek jakékoliv peněženky. V případě této diplomové práce mě vždy zajímá parametr confirmed_balance, jelikož parametr unconfirmed_balance obsahuje zůstatek, který není zatím v síti potvrzen.


```
{
  "status" : "success",
  "data" : {
    "network" : "BTC",
    "address" : "12wtQCtZVoThvypg6TJ3xSMBwDPLUTHBAi",
    "confirmed_balance" : "1.12600000",
    "unconfirmed_balance" : "3.56000000"
  }
}
```


Výpis 20: Odpověď z REST API Chain.so - Zůstatek Bitcoin peněženky [36]

V případě transakce, jak už bylo zmíněno, byla využita knihovna NBitcoin, která však pouze vygeneruje hexadecimální kód (hexadecimální reprezentace transakce), který je potřeba odeslat do Bitcoin sítě. Pro samotné odeslání bylo tedy opět využito RESTového API služby Chain.so, která toto umožňuje. Samotná služba zajistí to, že bude transakce rozeslána k ověření a následně zařazena do blockchainu [39]. Kód je tudíž rozdělen do tří částí, a to zjištění pohybu dané peněženky (UTXO), vytvoření transakce a získání transakce v podobě hexadecimální reprezentace transakce a odeslání transakce pomocí Chain.so API.

```
string url = $"https://chain.so/api/v2/get_tx_unspent/BTC/{address}";
using (WebClient wc = new WebClient())
  {
   var json = await wc.DownloadStringTaskAsync(url);
   List<LitecoinUTXO> utxos = JObject.Parse(json).GetValue("data").Value<
       JObject>().GetValue("txs").ToObject<List<LitecoinUTXO>>();
    return utxos;
  }
```

Výpis 21: Odpověď z REST API Chain.so - Získání UTXOS (Bitcoin)

Na ukázce kódu níže lze vidět vytvoření nové Bitcoin transakce v rámci jeho hlavní sítě a přiřazení historie pohybů (UTXO) jako vstup transakce.

```
Network network = NBitcoin.Network.Main;
BitcoinSecret bitcoinFrom = new BitcoinSecret(fromSecret, network);
NBitcoin.Transaction bitcoinTransaction = NBitcoin.Transaction.Create(network);

if (utxos.Count > 0)
   {
     foreach (LitecoinUTXO utxo in utxos)
       {
         var input = new TxIn();
         input.PrevOut = new OutPoint(new uint256(utxo.txid), 0);
         input.ScriptSig = bitcoinFrom.ScriptPubKey;
         bitcoinTransaction.Inputs.Add(input);
        }

   }
```

Výpis 22: NBitcoin - vytvoření nové transakce (Bitcoin)

```
var destination = BitcoinAddress.Create(toAddress, network);
var output = new TxOut();
Money fee = Money.Satoshis(35000); // Poplatek síti
output.Value = Money.Coins(amout) - fee;
output.ScriptPubKey = destination.ScriptPubKey;

bitcoinTransaction.Outputs.Add(output);
bitcoinTransaction.Sign(bitcoinFrom, false);

string hex = bitcoinTransaction.ToHex();
```

Výpis 23: NBitcoin - vygenerování HEX transakce

```
var values = new Dictionary<string, string>
{
  { "tx_hex", hex }
};
var content = new FormUrlEncodedContent(values);
var response = await client.PostAsync("https://chain.so/api/v2/send_tx/BTC",
    content);
var responseString = await response.Content.ReadAsStringAsync();

var txid = JObject.Parse(responseString).GetValue("data").Value<JObject>().
    GetValue("txid").Value<string>();
```

Výpis 24: Chain.so - odeslání Bitcoin transakce do sítě

Litecoin:

Pro implementaci Litcoinu byla využita, stejně jako v případě Bitcoinu, knihovna NBitcoin. Vzhledem k tomu, že je Litecoin vytvořen na základě technologie Bitcoinu, tak jej tato knihovna také podporuje. Implementace je opravdu velice podobná ne-li identická, a z tohoto důvodu zde nebude popsána. Jediné, co je potřeba v rámci kódu provést, je v případě REST API Chain.so v url nahradit BTC za LTC. V případě knihovny NBitcoin poté stačí změnit pouze network.

```
Network network = NBitcoin.Altcoins.Litecoin.Instance.Mainnet;
```

Výpis 25: NBitcoin - Litecoin network

Ethereum:
V případě implementace kryptoměny Ethereum byla v rámci diplomové práce využita .NET knihovna Nethereum (https://github.com/Nethereum/Nethereum). Implementovány byly opět tři funkce, a to vygenerování nové peněženky, transakce a zjištění zůstatku v peněžence. V případě této implementace na rozdíl od Bitcoinu a Litecoinu nebylo využito REST API služby Chain.so, jelikož tato služba podporuje pouze kryptoměny, které jsou založené na technologii Bitcoin. Na ukázce kódu níže je vidět vygenerování nové Ethereum peněženky. K tomuto vygenerování je potřeba náhodná sekvence znaků a několik slov. Tyto dva parametry slouží k vygenerování opravdu náhodné peněženky s nulovou šancí duplicit.

```
string Words = "ripple scissors kick mammal hire column oak again sun offer
    wealth tomorrow wagon turn fatal";
string Password = RandomString(10);
var wallet = new Wallet(Words, Password);

string[] address = wallet.GetAddresses(1);
string secret = wallet.GetAccount(address[0]).PrivateKey;
```

Výpis 26: Nethereum - Vygenerování nové Ethereum peněženky

```
Account ethereumAccount = new Account("d6X6dd6f6c9Efc69D11cX95c");
var web3 = new Web3(ethereumAccount);
TransactionReceipt transaction = await web3.Eth.GetEtherTransferService()
            .TransferEtherAndWaitForReceiptAsync("0
               x3E04c374FA457b6E05305f3bf0fF154b7AF42", 0.01m);
```

Výpis 27: Nethereum - Odeslání Etherea do jiné peněženky

```
var web3 = new Web3("https://mainnet.infura.io");
var balance = await web3.Eth.GetBalance.SendRequestAsync("0
    x3E04ce78374FA4575305f3bf0fF154b7AF42");
decimal etherAmount = Web3.Convert.FromWei(balance.Value);
```

Výpis 28: Nethereum - Zjíštění zůstatku Ethereum peněženky

NEO:

V případě předchozích kryptoměn byla pro implementaci využita .NET knihovna a ani kryptoměna NEO není výjimkou. Pro implementaci kryptoměny NEO byla využita .NET knihovna Neo lux (https://github.com/CityOfZion/neo-lux), která umožňuje provádět základní operace v rámci této kryptoměny.

```
byte[] privateKey = new byte[32];
using (RandomNumberGenerator rng = RandomNumberGenerator.Create())
{
   rng.GetBytes(privateKey);
}
KeyPair keys = new KeyPair(privateKey);
return (keys.address, keys.WIF);
```

Výpis 29: Neo lux - Vygenerování nové NEO peněženky

```
var keyStr = "SECRET";
var outputAddress = "AYVYDKH3kRnZJttY2DU78isQjY57vSL5q7";
var symbol = "NEO";
var fromKey = keyStr.Length == 52 ? KeyPair.FromWIF(keyStr) : new KeyPair(
    keyStr.HexToBytes());
NeoAPI api = NeoRPC.ForMainNet();
global::Neo.Lux.Core.Transaction tx = null;
if (api.IsToken(symbol))
{
   var token = api.GetToken(symbol);
   tx = token.Transfer(fromKey, outputAddress, amount);
} else if (api.IsAsset(symbol))
{
   tx = api.SendAsset(fromKey, outputAddress, symbol, amount);
}
```

Výpis 30: Neo lux - Transakce v rámci kryptoměny NEO

```
NeoRPC api = NeoRPC.ForMainNet();
var redPulse = api.GetUnspent("AYVYDKH3kRnZJttY2DU78isQjY57vSL5q7");
decimal balance = redPulse.Count > 0 ? redPulse.First(x => x.Key == "NEO").
    Value.Sum(x => x.value) : 0;
```

Výpis 31: Neo lux - Zjištění zůstatku peněženky NEO

Ripple:

Jak už bylo zmíněno na začátku této kapitoly, tak v případě Ripple se vyskytl problém s vygenerováním peněženky v rámci .NET. Tento problém jsem vyřešil tak, že vygenerování Ripple peněženky jsem implementoval v rámci jiného programovacího jazyka, a to konkrétně node.js, ve kterém je naprogramována frontend aplikace. Technicky je to tedy vyřešeno, tak že frontend aplikace obsahuje jednu veřejnou API funkci, která po zavolání v rámci .NET kódu vygeneruje novou ripple peněženku. V případě generování nové transakce byla využita volně dostupná .NET knihovna Ripple.NET (https://github.com/chriswill/ripple-netcore). Naopak pro zjištění stavu peněženky bylo využito volání oficiálního Ripple REST API, které je volně dostupné pro všechny vývojáře zdarma.

```
using (WebClient wc = new WebClient())
{
var json = await wc.DownloadStringTaskAsync($"http://localhost:3000/generate/
    wallet/XRP");
string WalletSecret = JObject.Parse(json).GetValue("secret").Value<string>();
string WalletId = JObject.Parse(json).GetValue("address").Value<string>();
}
```

Výpis 32: Node.js - Vygenerování nové Ripple peněženky

```
var secret = fromSecret;
var unsignedTxJson = @"{
   'Account': '" + fromAddress + @"',
   'Amount': '" + amout + @"',
   'Destination': '" + toAddress + @"',
   'Fee': '10',
   'Flags': 2147483648,
   'Sequence': 1,
   'TransactionType' : 'Payment'
}";
var signed = TxSigner.SignJson(JObject.Parse(unsignedTxJson), secret);
IRippleClient client = new RippleClient("wss://s1.ripple.com:443");
client.Connect();
SubmitBlobRequest request = new SubmitBlobRequest();
request.TransactionBlob = signed.TxBlob;
Submit result = await client.SubmitTransactionBlob(request);
client.Disconnect();
```

Výpis 33: Ripple.NET - Transakce v rámci kryptoměny Ripple

```
using (WebClient wc = new WebClient())
{
   var json = await wc.DownloadStringTaskAsync($"https://data.ripple.com/v2/
       accounts/{address}/balances?currency=XRP");
   var confirmedBalance = JObject.Parse(json).GetValue("balances").Value<JArray
       >();
   decimal balance = 0;
   foreach (JObject val in confirmedBalance)
   {
      balance += val.GetValue("value").Value<decimal>();
   }
}
```

Výpis 34: Ripple API - Zjištění zůstatku peněženky Ripple

DASH:

Při implementaci poslední z kryptoměn byla použita knihovna NBitcoin stejně jako tomu bylo u kryptoměn Bitcoin a Litecoin. Důvodem je to, že je kryptoměna opět založena na technologii Bitcoinu, a tudíž i implementace všech funkcí je opět stejná, jako tomu bylo u Bitcoinu. Stejně jako u Litecoinu stačí změnit network na DASH a všechny klíčová slova BTC v případě Chain.so na DASH.

```
Network network = NBitcoin.Altcoins.Dash.Instance.Mainnet;
```

Výpis 35: NBitcoin - Dash network

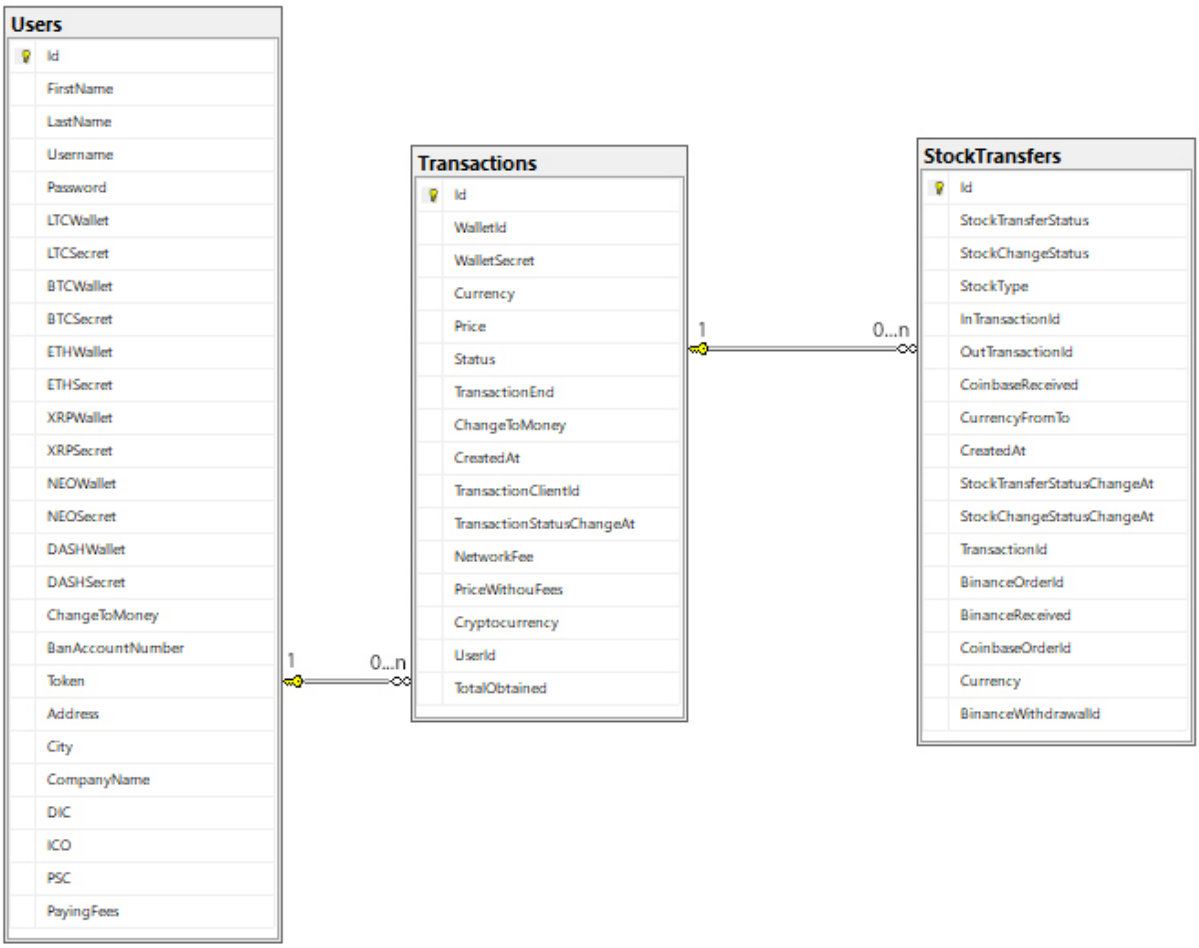
V této kapitole byla tedy popsána kompletní implementace všech kryptoměn, které jsem se rozhodl v rámci této diplomové práce podporovat. Ve všech případech byly využity knihovny, které implementaci jistým způsobem zjednodušily. V opačném případě by „čistá“ implementace těchto kryptoměn vyžadovala pro násobně mnoho času. Zároveň většina těchto knihoven neobsahuje dostatečnou dokumentaci, a tudíž bylo potřeba vyhledávat samotnou implementaci přímo v kódu knihoven. Tento fakt je způsoben tím, že většinou se jedná o čistě komunitní knihovny a jak je známo, komunita v případě .NET nefunguje, tak dobře, jako například v případě node.js kde takovéto knihovny existují, a ve většině případů jsou dobře popsány.

8.6 Technická implementace REST API a jeho popis

V rámci této diplomové práce byla pro implementaci backend aplikace využita ASP.NET Core 2.1. Jedná se o nejnovější verzi známého ASP.NET frameworku, který zde existuje již několik let a je v něm napsáno tisíce aplikací. Verze s označením Core oproti svému předchůdci může fungovat také v rámci operačního systému Linux nebo Mac. Jedná se o kompletně přepracovanou a odlehčenou architekturu, která ale obsahuje vše, co vývojář dnes potřebuje.

Vzhledem k tomu, že platební bránu ve většině případů využívá třetí strana, což je většinou nějaký e-shop. Rozhodl jsem zpřístupnit funkce aplikace pomocí dnes nejpoužívanější architektury REST API.

V případě databáze byl využit Microsoft SQL Server, ke kterému přistupuji a provádím všechny úkony pomocí knihovny Entity framework core. Samotné schéma databáze je znázorněno na obrázku č.27. Tabulka Transactions slouží k záznamu jednotlivých transakcí. Tabulka Users obsahuje registrované uživatele. Historie všech převodů mezi peněženkou a Binance, nebo Coinbase je zaznamenána v tabulce StockTransfers.



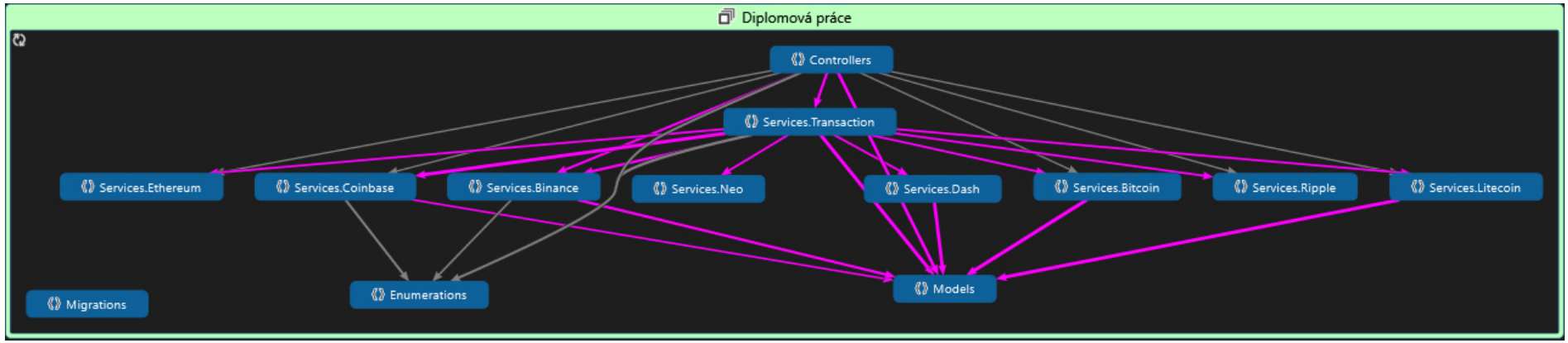
Obrázek 27: Databázové schéma

Aplikace je rozčleněna do několika oddělených části a to Controller, Model, Services. Controller je vstupní branou HTTP požadavku, kde při dotazu na danou URL určím, která servica se má zavolat. Services tedy obsahují logiku chceme-li „algoritmus“, který provádí různé úkony od generování peněženek po vložení údajů do databáze. Vložení do databáze se provádí pomocí entity frameworku, a to konkrétně vytvořením instance daného modelu, kde každý model je reprezentací jedné tabulky v databázi. Po vytvoření instance modelu a nastavení hodnot jeho parametrů je model uložen pomoci entity frameworku do databáze. Na těchto třech základních pilířích je aplikace postavena. Samozřejmě jsou zde ještě využívány například migrace pro jednodušší úpravu schémata databáze anebo enumerationy, což jsou statické číselníky, které slouží například k nastavení stavu platby. Aby nebylo potřeba v každém controlleru vytvářet instanci každé servicy zvlášť, je v rámci aplikace využit Dependendy injection. Ten je nastavený tak, aby každou třídu jejíž název končí slovem Service zaregistroval v rámci aplikace jako singleton instanci. Díky tomu stačí v rámci controlleru a jejího konstruktoru jako parametr zavolat danou třídu a nastavit ji jako instanční proměnnou daného controlleru.

```
// Startup.cs
services.RegisterAssemblyPublicNonGenericClasses(
   Assembly.GetExecutingAssembly())
.Where(c => c.Name.EndsWith("Service"))
.AsPublicImplementedInterfaces();
```

Výpis 36: ASP.NET Core - Automatický dependency injection

Aplikace obsahuje Controllery, které mají na starost například založení nové platby, autentizaci uživatele nebo kurzovní lístek. Každá kryptoměna má poté svou Servicu stejně jako ji má i Binance a Coinbase. Aplikace tedy obsahuje několik samostatných service. Každá tato servica se poté stará o práci s jednotlivými kryptoměnami a službami.



Obrázek 28: Visual studio - Code map

TransactionController:
Transaction controller se stará o akce spojené se samotnou transakcí. To znamená, že zajišťuje například vytváření nebo kontrolu stavu dané transakce. Tento controller je přístupný pouze přihlášeným uživatelům.

URL akce: POST api/transaction/createTransaction
Popis: Tato akce slouží k vytvoření nové transakce pro kryptoměnu uvedenou v parametru. Funkce při každém zavolání vytvoří v databázi novou transakci a vygeneruje příslušnou peněženku pro přijetí platby. Tato funkce je přístupná pouze pro přihlášené uživatele tzn. HTTP dotaz obsahuje bearer token.
Parametry:

Tabulka 12: API parametry - vytvoření transakce

Název	Datový typ	Povinný	Poznámka
cryptocurrency	Cryptocurrency	Ano	Kryptoměn podle hodnoty z číselníku
price	Double	Ano	Cena v EUR, nebo USD podle hodnoty currency
currency	Currency	Ano	Měna podle hodnoty číselníku

Odpověď:


```
{
    "id": 99,
    "walletId": "LUaXmv1CLV2YF9M2dXVnrtdwSpVe85Bzpy",
    "transactionEnd": "2019-04-09T18:42:57.6108046+02:00",
    "status": 2,
    "cryptocurrency": 2,
    "price": 0.0726,
    "priceWithouFees": 0.0691,
    "currency": "LTC",
    "createdAt": "2019-04-09T18:22:58.6168677+02:00",
    "transactionStatusChangeAt": "2019-04-09T18:22:58.616929+02:00",
    "changeToMoney": true,
    "networkFee": 0.03,
    "stockTransfers": null,
    "userId": 2
}
```


Výpis 37: API - odpověď po vytvoření transakce

URL akce: GET api/transaction/getTransactionInfo?transactionId=:transactionId
Popis: Akce slouží ke zjištění aktuálního stavu transakce. Na pozadí tato funkce mimo jiné ověřuje, zda jsou prostředky v dané peněžence a na základě těchto údajů stav této transakce mění. V případě, že peněženka obsahuje požadovanou částku, tak je transakce označena příslušným stavem. Tento stav udává například to, jestli je transakce momentálně ve stavu převodu na burze Binance nebo prodeje ve směnárně Coinbase. V případě, že je převod hotový funkce označí transakci jako hotovou a neprovádí s ní již další kroky. V případě, že by nebylo dodáno id transakce jsou kontrolovány všechny transakce, které jsou momentálně ve stavu zpracovávání. Vzhledem k tomu, že tato funkce má na starost kontrolu všech stavů a zahájení všech procesů výměny, je potřeba ji volat v určitých intervalech ať už na straně samotné platební brány nebo na straně zákazníka (e-shopu). Akce je přístupná pouze přihlášenému uživateli, který v HTTP dotazu obsáhl bearer token.
Parametry:

Tabulka 13: API parametry - získání info o transakci

Název	Datový typ	Povinný	Poznámka
:transactionId	Integer	Ano	Id transakce

Odpověď:

```
{
    "id": 99,
    "walletId": "LUaXmv1CLV2YF9M2dXVnrtdwSpVe85Bzpy",
    "transactionEnd": "2019-04-09T18:42:57.6108046+02:00",
    "status": 1,
    "cryptocurrency": 2,
    "price": 0.0726,
    "priceWithouFees": 0.0691,
    "currency": "LTC",
    "createdAt": "2019-04-09T18:22:58.6168677+02:00",
    "transactionStatusChangeAt": "2019-04-09T19:15:18.616929+02:00",
    "changeToMoney": true,
    "networkFee": 0.03,
    "stockTransfers": null,
    "userId": 2
}
```

Výpis 38: API - odpověď funkce getTransactionInfo

ExchangeRateController:
Exchange rate controller se stará o zjištění cen v rámci všech podporovaných kryptoměn. Slouží primárně pro živý kurzovní lístek.

URL akce: GET api/exchange-rate/getPrices?currency=:currency
Popis: Tato akce slouží k vrácení ceny všech podporovaných kryptoměn v rámci platební brány. Akce je vytvořena především pro zobrazení živého kurzovního lístku. Akce je přístupna i neregistrovaným uživatelům.
Parametry:

Tabulka 14: API parametry - funkce getPrices

Název	Datový typ	Povinný	Poznámka
:currency	Integer	Ano	USD nebo EUR

Odpověď:

```
[
    {
        "cryptoName": "Bitcoin",
        "cryptoSign": "BTC",
        "currencySign": "USD",
        "price": 7082.1728
    },
    {
        "cryptoName": "Litecoin",
        "cryptoSign": "LTC",
        "currencySign": "USD",
        "price": 94.3504
    },
    {
        "cryptoName": "Ripple",
        "cryptoSign": "XRP",
        "currencySign": "USD",
        "price": 0.478542416096
    }
    ...
]
```

Výpis 39: API - odpověď API funkce gerPrices

Tabulka 15: Statické číselníky (Enumerations)

TransactionStatus		
0	Done	Transakce hotova
1	Expired	Transakce vypršela
2	Waiting	Transakce v čekajícím stavu
3	TransferedToStockMarket	Prostředky převedeny na burzu
4	TransferedToCoinbase	Prostředky převedeny na Coinbase
5	TransferedToBankAccount	Peníze odeslány na bankovní účet
StockTransferStatus		
0	Done	Převod hotov
1	Transfering	Převod probíhá
2	TransferedAndPendig	Převedeno a čeká na potvrzení
3	TransferedAndCompleted	Převedeno a potvrzeno
StockChangeStatus		
0	Done	Výměna hotova
1	Changing	Výměna probíhá
Cryptocurrency		
0	BTC	-
1	ETH	-
2	LTC	-
3	XRP	-
4	NEO	-
5	DASH	-
Currency		
0	EURO	-
1	USD	-
CurrencyFromTo		
0	LitecoinEURO	-
1	EthereumEURO	-
2	BitcoinEURO	-
3	LitecoinUSD	-
4	EthereumUSD	-
5	BitcoinUSD	-
6	RippleBTC	-
7	NeoBTC	-
8	DashBTC	-
StockType		
0	Binance	-
1	Coinbase	-

8.7 Zabezpečení

Jelikož aplikace v rámci této diplomové práce pracuje s financemi, je nutné ji také patřičně zabezpečit. Největším rizikem je v tomto případě ukradení přístupových údajů k práci se směnárnou Coinbase a burzou Binance. V tomto případě by se mohlo stát, že útočník odcizí přístupové klíče, pomocí kterých by byl schopen například převést všechny směněné prostředky na své účty. Druhým rizikem je ukládání klíčů ke kryptoměnovým peněženkám, které jsou v rámci aplikace generovány. Na těchto peněženkách budou v jednom momentě vždy nějaké prostředky, a v případě odcizení těchto klíčů by útočník mohl získat neomezený přístup k peněžence, a tím pádem možnost odcizit její obsah.

V prvním případě je tedy potřeba zabezpečit přístupové klíče k práci s REST API Binance a Coinbase. Tyto klíče musí být zabezpečeny v rámci aplikace, jelikož je není potřeba mít uložené například v databázi. V rámci této diplomové práce bylo využito již zabudovaného zabezpečení v rámci ASP.NET Core, které se nazývá secret storage. Tento způsob sice není stoprocentní, jelikož samotná hesla ukládá v nezašifrované podobě, ale ve většině případů to stačí, jelikož tyto údaje útočník odcizí pouze v případě přístupu na server. Navíc v tomto případě už většinou vývojáře nezachrání nic. Jde tedy o to, aby klíče neobsahovala aplikace samotná pro případ, kdyby někdy útočník získal přístup ke zdrojovým kódům aplikace.

Druhým případem je způsob ukládání klíčů k peněženkám, které byly vygenerovány v rámci aplikace. Tyto klíče je potřeba ukládat do databáze. V rámci aplikace jsou klíče ukládané do databáze šifrovány a při čtení dešifrovány. Toto zabezpečení zajistí, že v případě, kdy útočník odcizí data z databáze, tak stejně nebude schopen klíče přečíst, a tudíž jsou mu k ničemu. Tyto údaje by mu byly dobré pouze v případě, pokud zjistí, jakým způsobem jsou klíče šifrovány.

Vzhledem k tomu, že aplikaci momentálně neplánuji využít v reálném provozu, není potřeba zabezpečovat server. V rámci této diplomové práce byla aplikace nasazena na hostovaný cloud serveru, u kterého se o zabezpečení stará konkrétní poskytovatel této služby. V případě vlastního serveru bych určitě podrobně prozkoumal všechny zranitelnosti, a to především Linux serveru, který by byl případně pro běh aplikace využit.

9 Závěr

Cílem této diplomové práce bylo analyzovat a implementovat platební bránu, která bude kromě klasických kryptoměn přijímat také kryptoměny alternativní. Z tohoto důvodu jsem čtenáře na úvod této diplomové práce seznámil s tím, co to kryptoměny jsou, jak je získat, co je to Bitcoin a co to jsou alternativní kryptoměny. V další kapitole byla popsána bezpečnost v rámci kryptoměn a zodpovězena otázka, jestli jsou kryptoměny bezpečné, jak se vůbec chránit a jestli kryptoměny opravdu zaručují anonymitu. Kapitola 4 byla následně zaměřena na burzy kryptoměn, jejich poplatky a omezení, nebo obecně na trhy s kryptoměnami. Tato kapitola slouží především ke zjištění, jaké burzy existují, a jak funguje trh s kryptoměnami. Vzhledem k tomu, že cílem této diplomové práce bylo navrhnout a vytvořit platební bránu, rozhodl jsem se popsat největší platební brány v rámci světa a České republiky. V další kapitole byly popsány momentálně dostupné kryptoměnové platební brány. Vzhledem k požadavkům registrace však nebylo možné je otestovat. Tato analýza však stačila k tomu, abych si uvědomil, jak tyto brány vlastně v praxi fungují. Poslední kapitolou v rámci teoretické části byly kapitola č.7 o legislativním rámci ve vztahu ke kryptoměnám v EU a České republice. Tato kapitola se zaměřuje na to, jak jsou kryptoměny brány z pohledu legislativy u nás a v Evropské unii.

Kapitola č.8 se zabývala implementací konkrétního řešení vlastní kryptoměnové platební brány. Na začátku této kapitoly je popsáno, jak by měla a bude platební brána fungovat. V rámci této části jde především o myšlenku fungování brány, tak aby bylo srozumitelné, jak brána bude fungovat. Následně byl v podkapitole 8.2 vysvětlen postup implementace a zároveň také popsány problémy, se kterými jsem se musel vypořádat. Z tohoto důvodu bylo potřeba se z mé strany podrobně seznámit s funkcionalitou všech implementovaných kryptoměn, tak abych byl schopen implementaci provést. V další podkapitole poté byla popsána implementace mnou zvolené burzy pro výměnu altcoinů, což jsou v tomto případě kryptoměny Ripple, DASH a NEO. Popisuji především implementované funkce, které Binance poskytuje prostřednictvím REST API a popisuji jejich funkcionalitu včetně REST API parametrů a odpovědí. V následující podkapitole popisuji taktéž REST API funkce, které jsem v aplikaci využil u směnárny Coinbase. V rámci těchto dvou kapitol jsem také využil ukázky reálného kódu tak, aby bylo zřejmé, jak implementace vypadá. V další podkapitole poté popisuji samotnou implementaci všech zvolených kryptoměn, a to především pomocí ukázek reálného kódu přímo z aplikace. Tato část byla v rámci programování aplikace tou nesložitější, jelikož se bylo potřeba seznámit s funkcionalitou těchto kryptoměn. V předposlední podkapitole popisuji implementaci vlastního REST API, které slouží k založení a sledování stavu plateb v rámci platební brány. V závěrečné podkapitole jsem se zaměřil na zabezpečení samotné aplikace a s tím, které konkrétní kroky byly v rámci platební brány provedeny.

Samotná implementace dopadla dle předpokladů dobře, což znamená, že se mi povedlo vytvořit platební bránu, díky které jsem schopen například v rámci vlastního e-shopu podporovat platby pomoci známých kryptoměn jako je Bitcoin, Litecoin nebo Ethereum a zároveň také pomocí méně známých, ale neméně důležitých altcoinů Ripple, Dash a NEO. Výstupem této diplomové práce je tedy jakýsi „návod“, jak takovouto platební bránu sestrojit. Samozřejmě je zde prostor pro případná další rozšíření, a to například přidáním podpory dalších kryptoměn v rámci platební brány, nebo také implementace více burz, které zajistí nejlepší možnou cenu v rámci směny kryptoměn na Bitcoin. Také je zde prostor k vylepšení stávajícího algoritmu, tak aby popřípadě mohla být platební brána využita v reálném provozu jako konkurence pro již fungující platební brány. V porovnání s již existujícími platebními branami toto řešení z pohledu procesu platby funguje velice podobně. Výhodou oproti ostatním by ale každopádně měla být výše poplatků za platbu. V případě implementace vlastního řešení platební brány v rámci svého e-shopu majitel určitě ušetři nemalé peníze na poplatcích, které si většinou kromě směnáren a burz účtují také samotné platební brány. Samozřejmě je zde také prostor pro vytvoření vlastního produktu v podobě platební brány, kterou by bylo možno nabízet e-shopům stejně jako to například již nyní děla Bitcoinpay.

Literatura

[1] *What is Cryptocurrency: Everything You Must Need To Know!* [online]. [cit. 2018-11-05]. Dostupné z: https://blockgeeks.com/guides/what-is-cryptocurrency/

[2] *What is Cryptocurrency: Everything You Must Need To Know!* [online]. [cit. 2018-11-05]. Dostupné z: https://www.thestreet.com/investing/bitcoin/bitcoin-history-14686578

[3] *Altcoin* [online]. [cit. 2018-11-05]. Dostupné z: https://www.investopedia.com/terms/a/altcoin.asp

[4] *Ripple (VŠE CO CHCETE VĚDĚT)* [online]. [cit. 2018-11-05]. Dostupné z: https://www.alza.cz/ripple-xrp

[5] *Dash - kryptoměna zajímavá pro mining i inovátory* [online]. [cit. 2018-11-05]. Dostupné z: https://www.e15.cz/dash-coin-kurz-mining-wiki

[6] *1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do* [online]. [cit. 2018-11-05]. Dostupné z: https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html

[7] *Research: More than 56% of all cryptocurrency crime happens in the US* [online]. [cit. 2018-11-05]. Dostupné z: https://thenextweb.com/hardfork/2018/08/06/cryptocurrency-crime-statistics-hacks/

[8] *Bitcoin and Cryptocurrencies: Are They Safe?* [online]. [cit. 2018-11-05]. Dostupné z: https://www.experian.com/blogs/ask-experian/bitcoin-and-cryptocurrencies-are-they-safe/

[9] *Coincheck Hack: "The Biggest Theft in the History of the World"* [online]. [cit. 2018-11-05]. Dostupné z: https://cryptonews.com/news/coincheck-hacked-more-than-500-million-xem-stolen-1093.htm

[10] *8 Steps to Protecting Your Cryptocurrency* [online]. [cit. 2018-11-05]. Dostupné z: https://decryptionary.com/what-is-cryptocurrency/8-steps-protecting-cryptocurrency/

[11] *Anonymity of cryptocurrencies* [online]. [cit. 2018-11-05]. Dostupné z: https://anoncoin.net/Anonymity_of_cryptocurrencies/

[12] *13 Top Best Bitcoin/Cryptocurrency Exchanges (2019 Reviews)* [online]. [cit. 2018-11-05]. Dostupné z: https://www.bitpremier.com/best-exchanges

[13] *Binance - Fee Schedule* [online]. [cit. 2018-11-05]. Dostupné z: https://www.binance.com/en/fee/schedule

[14] *Coinbase Pricing & Fees Disclosures* [online]. [cit. 2018-11-05]. Dostupné z: https://support.coinbase.com/customer/en/portal/articles/2109597-coinbase-pricing-fees-disclosures

[15] *Spot Trade, Stable Coin & Dark Pool Trading Fee Structures | Kraken* [online]. [cit. 2018-11-05]. Dostupné z: https://www.kraken.com/en-us/features/fee-schedule

[16] *Fees and charges - Coinmama* [online]. [cit. 2018-11-05]. Dostupné z: https://support.coinmama.com/hc/en-us/articles/213577065-Fees-and-charges

[17] *What fees can I expect to pay? & Bitpanda Helpdesk* [online]. [cit. 2018-11-05]. Dostupné z: https://support.bitpanda.com/hc/en-us/articles/360000902525-What-fees-can-I-expect-to-pay-

[18] *Fee schedule - CEX.IO* [online]. [cit. 2018-11-05]. Dostupné z: https://cex.io/fee-schedule#/tab/payments

[19] *Fee Schedule - Bitstamp* [online]. [cit. 2018-11-05]. Dostupné z: https://www.bitstamp.net/fee_schedule/

[20] *FAQ | Changelly.com* [online]. [cit. 2018-11-05]. Dostupné z: https://changelly.com/faq

[21] *Trading Fee Schedule* [online]. [cit. 2018-11-05]. Dostupné z: https://gemini.com/trading-fee-schedule/#trading-fee-schedule

[22] *Bitfinex - Our fees* [online]. [cit. 2018-11-05]. Dostupné z: https://www.bitfinex.com/fees

[23] *Understanding the Cryptocurrency Market - Blockchain Technology Explained | Toptal* [online]. [cit. 2018-11-05]. Dostupné z: https://www.toptal.com/finance/market-research-analysts/cryptocurrency-market

[24] *Právní regulace kryptoměn v ČR* [online]. [cit. 2018-11-05]. Dostupné z: https://sb-sb.cz/cz/news/pravovoe-regulirovanie-kriptovalyut-v-chehii

[25] *Přednáška VŠE* [online]. [cit. 2018-11-05]. Dostupné z: https://kpu.vse.cz/wp-content/uploads/2018/03/P%C5%99edn%C3%A1%C5%A1ka_VSE_final.pdf

[26] *Cryptocurrency Regulation In The European Union* [online]. [cit. 2018-11-05]. Dostupné z: https://cryptobriefing.com/cryptocurrency-regulation-european-union/

[27] *Bitcoin – Google Trends* [online]. [cit. 2018-11-05]. Dostupné z: https://trends.google.com/trends/explore?date=2010-01-01%202019-02-25&geo=US&q=Bitcoin

[28] *Litecoin – Google Trends* [online]. [cit. 2018-11-05]. Dostupné z: https://trends.google.com/trends/explore?date=2010-01-01%202019-02-25&geo=US&q=Litecoin

[29] *Ethereum – Google Trends* [online]. [cit. 2018-11-05]. Dostupné z: https://trends.google.com/trends/explore?date=2010-01-01%202019-02-25&geo=US&q=Ethereum

[30] *Ripple – Google Trends* [online]. [cit. 2018-11-05]. Dostupné z: https://trends.google.com/trends/explore?date=2010-01-01%202019-02-25&geo=US&q=Ripple

[31] *Dash – Google Trends* [online]. [cit. 2018-11-05]. Dostupné z: https://trends.google.com/trends/explore?date=2010-01-01%202019-02-25&geo=US&q=%2Fm%2F010rcq2_

[32] *NEO cryptocurrency – Google Trends* [online]. [cit. 2018-11-05]. Dostupné z: https://trends.google.com/trends/explore?date=2010-01-01%202019-02-25&geo=US&q=NEO%20cryptocurrency

[33] *API Documentation (REST and Realtime)* [online]. [cit. 2018-11-05]. Dostupné z: https://chain.so/api

[34] *Infura - Scalable Blockchain Infrastructure* [online]. [cit. 2018-11-05]. Dostupné z: https://infura.io/docs

[35] *rippled API Reference* [online]. [cit. 2018-11-05]. Dostupné z: https://developers.ripple.com/rippled-api.html

[36] *Chain.so - stav Bitcoin peněženky* [online]. [cit. 2018-11-05]. Dostupné z: https://chain.so/api/v2/get_address_balance/LTC/LZ5zpM9jot4VFAs9DTAsGgBZksvAWZ8sn8

[37] *Public Rest API for Binance* [online]. [cit. 2018-11-05]. Dostupné z: https://github.com/binance-exchange/binance-official-api-docs/blob/master/rest-api.md

[38] *NBitcoin* [online]. [cit. 2018-11-05]. Dostupné z: https://github.com/MetacoSA/NBitcoin

[39] *What is Blockchain Technology? A Step-by-Step Guide For Beginners* [online]. [cit. 2018-11-05]. Dostupné z: https://blockgeeks.com/guides/what-is-blockchain-technology/n

[40] *Bezpečné ukládání tajných kódů aplikace při vývoji v ASP.NET* [online]. [cit. 2018-11-05]. Dostupné z: https://docs.microsoft.com/cs-cz/aspnet/core/security/app-secrets?view=aspnetcore-2.2&tabs=windows